Docket No.: 67471-037 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Takio YAMASHITA	:	Confirmation Number:
Serial No.:	:	Group Art Unit:
Filed: March 17, 2004	:	Examiner:

For: DEBUG SYSTEM, MICROPROCESSOR, AND DEBUGGER

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicant hereby claim the priority of:

Japanese Patent Application No. JP 2003-076145, filed on March 19, 2003.

A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:gav
Facsimile: (202) 756-8087
Date: March 17, 2004

67471-037
Takio YAMASHITA
March 17, 2004

日本国特許庁 JAPAN PATENT OFFICE

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　３月１９日
出願番号 Application Number:	特願２００３－０７６１４５
[ST. 10/C]:	[ＪＰ２００３－０７６１４５]
出願人 Applicant(s):	松下電器産業株式会社

２００３年１２月１７日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３１０４７０６

【書類名】　特許願
【整理番号】　5037730155
【提出日】　平成15年 3月19日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/14
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　山下　太紀夫
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9003742
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　デバッグシステム、マイクロプロセッサ及びデバッガ

【特許請求の範囲】

【請求項１】　外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと、前記マイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするために用いられるホストコンピュータとから構成されるデバッグシステムであって、

前記マイクロプロセッサは、

前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の領域を備える一度だけ書き込みが可能な不揮発性メモリと、

前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、受け取った鍵情報を前記不揮発性メモリに書き込む書込手段と、

前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する第１伝送手段とを備え、

前記ホストコンピュータは、

利用者から鍵情報の入力を受け付ける受付手段と、

前記鍵情報を内部に記憶すると共に、前記マイクロプロセッサへ送出する送出手段と、

記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する第２伝送手段とを備える

ことを特徴とするデバッグシステム。

【請求項２】　デバッグするために用いられるホストコンピュータと接続され、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサであって、

プログラム、データ又はプログラム及びデータを示す前記プログラム情報を記憶しているプログラム情報記憶手段と、

前記プログラム情報を読み出し、読み出したプログラム情報に従って動作する実行手段と、

前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の

領域を備える一度だけ書き込みが可能な不揮発性メモリと、

前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、受け取った鍵情報を前記不揮発性メモリに書き込む書込手段と、

前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備える

ことを特徴とするマイクロプロセッサ。

【請求項３】　前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、

前記伝送手段は、前記フラグ情報を読み出し、読み出した前記フラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記ホストコンピュータから鍵情報を受け付け、受け付けた鍵情報を前記不揮発性メモリに書き込む

ことを特徴とする請求項２に記載のマイクロプロセッサ。

【請求項４】　前記伝送手段は、

前記不揮発性メモリに記憶されている鍵情報を用いて、前記プログラム情報を暗号化する暗号化部と、

暗号化されたプログラム情報を出力する出力部とを含む

ことを特徴とする請求項３に記載のマイクロプロセッサ。

【請求項５】　前記プログラム情報記憶手段は、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、

前記実行手段は、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、　生成したプログラム、データ又はプログラム及びデータに従って動作し、

前記伝送手段は、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を伝送する

ことを特徴とする請求項３に記載のマイクロプロセッサ。

【請求項６】　前記実行手段は、更に、動作の結果生成された生成データを、鍵情報を用いて暗号化し、暗号化された生成データを前記プログラム情報記憶手段に書き込む

ことを特徴とする請求項５に記載のマイクロプロセッサ。

【請求項７】　前記プログラム情報記憶手段は、前記プログラムのみが鍵情報を用いて暗号化された暗号化プログラムを含むプログラム情報を記憶しており、

前記プログラム情報記憶手段は、前記外部装置との通信経路を備える

ことを特徴とする請求項５に記載のマイクロプロセッサ。

【請求項８】　前記鍵情報は１以上の部分鍵情報から構成され、

前記プログラムは、複数の部分プログラムから構成され、各部分プログラムは、前記１以上の部分鍵情報の何れかに対応しており、

前記プログラム情報記憶手段は、複数の部分プログラムが、対応する部分鍵情報を用いて暗号化された暗号化部分プログラムを含むプログラム情報を記憶しており、

前記実行手段は、前記不揮発性メモリから部分鍵情報を読み出し、読み出した部分鍵情報に対応する１以上の暗号化部分プログラムをプログラム情報記憶手段から読み出し、読み出した１以上の暗号化部分プログラムを、前記部分鍵情報を用いて復号して部分プログラムを生成し、生成した部分プログラムに従って動作する

ことを特徴とする請求項５に記載のマイクロプロセッサ。

【請求項９】　前記伝送手段は、さらに、前記ホストコンピュータからの要求に応じて、前記出力部における暗号化されたプログラム情報の出力を抑制する抑制部を含む

ことを特徴とする請求項４に記載のマイクロプロセッサ。

【請求項１０】　前記伝送手段は、さらに、

鍵情報に係る情報で、前記出力部における暗号化されたプログラム情報の出力の抑制を示す抑制条件を記憶している抑制条件記憶部と、

前記ホストコンピュータから受け付けた前記鍵情報が、前記抑制条件を満たす場合に、前記出力部における前記出力を抑制する抑制部とを含む

ことを特徴とする請求項４に記載のマイクロプロセッサ。

【請求項１１】　前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、

前記伝送手段は、前記フラグ情報を読み出し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記プログラム情報記憶手段から前記プログラム情報を読み出し、読み出したプログラム情報を出力し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていることを示す場合に、前記プログラム情報記憶手段から前記プログラム情報を読み出し、読み出したプログラム情報を前記鍵情報で暗号化し、暗号化されたプログラム情報を出力する

ことを特徴とする請求項２に記載のマイクロプロセッサ。

【請求項１２】　前記マイクロプロセッサは、更に、キャッシュメモリを備え、

前記プログラム情報記憶手段は、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、

前記実行手段は、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成した前記プログラム、データ又はプログラム及びデータを前記キャッシュメモリに書き込み、前記実行手段の実行速度に応じて前記キャッシュメモリから前記プログラム、データ又はプログラム及びデーを読み出し、読み出したプログラム、データ又はプログラム及びデータに従って動作し、

前記伝送手段は、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を伝送する

ことを特徴とする請求項３に記載のマイクロプロセッサ。

【請求項１３】　外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするホストコンピュータであって、

利用者から鍵情報の入力を受け付ける受付手段と、

前記鍵情報を、内部に記憶すると共に前記マイクロプロセッサへ送出する送出手段と、

記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備える

ことを特徴とするホストコンピュータ。

【請求項１４】　前記伝送手段は、

前記マイクロプロセッサから、前記鍵情報を用いて暗号化されたプログラム情報を受け取るプログラム情報受取部と、

前記暗号化されたプログラム情報に、記憶している前記鍵情報を用いて復号する復号部と、

前記復号部が復号したプログラム情報を表示する表示部とを備える

ことを特徴とする請求項１３に記載のホストコンピュータ。

【請求項１５】　前記伝送手段は、更に、

利用者から、プログラム、データ又はプログラム及びデータを示すプログラム情報の入力を受け付けるプログラム情報入力部と、

受け付けた前記プログラム情報に、記憶している前記鍵情報を用いて暗号化する暗号部と、

前記暗号部が暗号化したプログラム情報を前記マイクロプロセッサへ出力する出力部とを備える

ことを特徴とする請求項１４に記載のホストコンピュータ。

【請求項１６】　前記ホストコンピュータは、更に、

ソースプログラムを記憶している記憶手段と、

前記ソースプログラムを変換してプログラムを示すプログラム情報を生成する変換手段と、

前記プログラム情報に、前記鍵情報を用いて暗号化する暗号化手段とを備え、

前記伝送手段は、前記暗号化手段が暗号化したプログラム情報を前記マイクロプロセッサへ伝送する

ことを特徴とする請求項１４に記載のホストコンピュータ。

【請求項１７】　前記伝送手段は、さらに、

鍵情報に係る情報で、前記マイクロプロセッサとの間での前記暗号化されたプログラム情報の伝送の停止を示す停止条件を記憶している停止条件記憶部と、

前記入力手段が受け付けた前記鍵情報が、前記停止条件を満たす場合に、前記マイクロプロセッサに対して、前記暗号化されたプログラム情報の出力を抑制することを示す要求　を出力する抑制要求出力部とを含む

ことを特徴とする請求項１４に記載のホストコンピュータ。

【請求項１８】　外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと接続されたリードライト装置であって、

利用者から鍵情報の入力を受け付ける受付手段と、

前記鍵情報を内部に記憶すると共に前記マイクロプロセッサへ送出する送出手段と、

記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備える

ことを特徴とするリードライト装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、マイクロプロセッサ及び前記マイクロプロセッサをデバッグする技術に関する。

【０００２】

【従来の技術】

昨今、ＩＣチップを搭載したＩＣカードが課金処理を扱うシステムで用いられるようになってきている。ＩＣチップは、マイクロプロセッサ、ＲＯＭ、ＲＡＭなどを備える微小なコンピュータシステムである。前記ＲＯＭには、制御用コンピュータプログラムが格納されており、前記マイクロプロセッサは制御用コンピュータプログラムを実行することにより、ＩＣカードの課金処理を制御する。

【０００３】

一方で、マイクロプロセッサは、設計後及び出荷後のデバッグを可能にするために、デバッグインターフェースを搭載している。デバッグとは、デバッグユニ

ットと接続されたホストパーソナルコンピュータ（以下「ホストＰＣ」と言う）上で動作するデバッガが、当該マイクロプロセッサ内部のメモリに格納された命令又はデータを抽出してホストＰＣ上に表示すること、及び、ホストＰＣ上で入力された命令又はデータをマイクロプロセッサのメモリに書き込むことにより、プログラムのバグを見つけて修正することである。

【０００４】

この様に、デバッグインターフェースを搭載しているマイクロプロセッサが、課金情報を扱うシステムで用いられるＩＣカードに搭載されると、悪意のある解析者に内部の命令及びデータを不正に解析、改竄される危険性があるため、このようなシステムで用いるマイクロプロセッサには、命令及びデータを解析、改竄されるのを防止するための高いセキュリティが要求される。

【０００５】

そこで、特許文献１によると、実行プログラムを内蔵したＲＯＭと前記ＲＯＭに前記実行プログラムを書き込む入出力装置と前記ＲＯＭから前記実行プログラムを読み出す半導体プロセッサとから構成される情報保護システムであって、暗号化した実行プログラムをＲＯＭに書き込み、暗号化された実行プログラムを前記ＲＯＭから読み出し、復号する技術が開示されている。

【０００６】

また、特許文献２によると、ＲＯＭに記録された情報を、外部に設けられたデバッグツールによる不正アクセスから保護する情報処理装置であって、ユーザにより個別に設定可能なセキュリティ解除プログラムを含み、外部に設けられたエミュレータによる不正アクセスから保護すべき情報を記憶するメモリと、前記エミュレータに接続されて、前記エミュレータと当該情報処理装置との間でデバッグに必要な信号の入出力制御を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路とを備え、電源投入時に前記情報処理装置をリセットするパワーオンリセット信号を受けて、前記オンチップデバッグ回路の機能を無効化してセキュリティを設定し、前記エミュレータによる前記メモリが記憶している前記情報の読み出しを禁止し、セキュリティ指定ビットと当該セキュリティ指定ビットのリセットをイネーブルとするイネーブルコードとを受けて、前記オ

ンチップデバッグ回路の機能を有効化してセキュリティを解除し、前記エミュレータによる、前記情報の読み出しを可能にする情報処理装置に関する技術が開示されている。

【０００７】

上記の様に、内部情報を保護するためにマイクロプロセッサに暗号化回路を設け、内部情報を暗号化して外部へ出力することが行われている。マイクロプロセッサは、設計時に設定されたキーコードを保持しており、このキーコードを用いて命令及びデータの暗号化を行う。ホストＰＣ上で動作するデバッガは、復号化回路を備え、前記マイクロプロセッサから暗号化された命令及びデータを受信し、前記キーコードの入力を受け付けて命令及びデータを復号する。従って、前記キーコードを知る者のみが正しく復号された命令及びデータを得てデバッグを行うことが出来る。

【０００８】

【特許文献１】

特開２０００－３５７０８５号公報

【０００９】

【特許文献２】

特開２０００－３４７９４２号公報

【００１０】

【発明が解決しようとする課題】

しかしながら、上記のマイクロプロセッサは、設計時にキーコードを書き込む為、当該キーコードはマイクロプロセッサ設計者やデバッガ設計者等のシステム開発者には既知である。課金情報を扱うシステムで用いられるＩＣカードを例に考えると、マイクロプロセッサ製造者とＩＣカード製造者とＩＣカード供給者とはそれぞれ異なる。マイクロプロセッサ製造者及びＩＣカード製造者は当該システムの利用者なり得るため、マイクロプロセッサにデバッグユニットを接続して内部情報を解読、改竄されかねないという問題がある。

【００１１】

本発明は、上記問題点に鑑みなされたものであって、マイクロプロセッサのデ

バッグと内部情報のセキュリティの確保とを両立できるマイクロプロセッサ、デバッガ及びデバッグシステムを提供することを目的とする。

【００１２】

【課題を解決するための手段】

上記目的を達成するために、本発明は、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと、前記マイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするために用いられるホストコンピュータとから構成されるデバッグシステムである。

【００１３】

前記マイクロプロセッサは、前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の領域を備える一度だけ書き込みが可能な不揮発性メモリと、前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、受け取った鍵情報を前記不揮発性メモリに書き込む書込手段と、前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する第１伝送手段とを備える。

【００１４】

前記ホストコンピュータは、利用者から鍵情報の入力を受け付ける受付手段と、前記鍵情報を内部に記憶すると共に、前記マイクロプロセッサへ送出する送出手段と、記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する第２伝送手段とを備える。

また、本発明は、デバッグするために用いられるホストコンピュータと接続され、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサである。前記マイクロプロセッサは、プログラム、データ又はプログラム及びデータを示す前記プログラム情報を記憶しているプログラム情報記憶手段と、前記プログラム情報を読み出し、読み出したプログラム情報に従って動作する実行手段と、前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の領域を備える一度だけ書き込みが可能な不揮発性メモリと、前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、

受け取った鍵情報を前記不揮発性メモリに書き込む書込手段と、前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備えることを特徴とする。

【００１５】

ここで、前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、前記伝送手段は、前記フラグ情報を読み出し、読み出した前記フラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記ホストコンピュータから鍵情報を受け付け、受け付けた鍵情報を前記不揮発性メモリに書き込むことを特徴とする。

【００１６】

ここで、前記伝送手段は、前記不揮発性メモリに記憶されている鍵情報を用いて、前記プログラム情報を暗号化する暗号化部と、暗号化されたプログラム情報を出力する出力部とを含むことを特徴とする。

また、前記プログラム情報記憶手段は、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、前記実行手段は、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成したプログラム、データ又はプログラム及びデータに従って動作し、前記伝送手段は、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を伝送することを特徴とする。

【００１７】

ここで、前記実行手段は、更に、動作の結果生成された生成データを、鍵情報を用いて暗号化し、暗号化された生成データを前記プログラム情報記憶手段に書き込むことを特徴とする。

ここで、前記プログラム情報記憶手段は、前記プログラムのみが鍵情報を用いて暗号化された暗号化プログラムを含むプログラム情報を記憶しており、前記プログラム情報記憶手段は、前記外部装置との通信経路を備えることを特徴とする。

【００１８】

また、前記鍵情報は１以上の部分鍵情報から構成され、前記プログラムは、複数の部分プログラムから構成され、各部分プログラムは、前記１以上の部分鍵情報の何れかに対応しており、前記プログラム情報記憶手段は、複数の部分プログラムが、対応する部分鍵情報を用いて暗号化された暗号化部分プログラムを含むプログラム情報を記憶しており、前記実行手段は、前記不揮発性メモリから部分鍵情報を読み出し、読み出した部分鍵情報に対応する１以上の暗号化部分プログラムをプログラム情報記憶手段から読み出し、読み出した１以上の暗号化部分プログラムを、前記部分鍵情報を用いて復号して部分プログラムを生成し、生成した部分プログラムに従って動作することを特徴とする。

【００１９】

また、前記伝送手段は、さらに、前記ホストコンピュータからの要求に応じて、前記出力部における暗号化されたプログラム情報の出力を抑制する抑制部を含むことを特徴とする。

また、前記伝送手段は、さらに、鍵情報に係る情報で、前記出力部における暗号化されたプログラム情報の出力の抑制を示す抑制条件を記憶している抑制条件記憶部と、前記ホストコンピュータから受け付けた前記鍵情報が、前記抑制条件を満たす場合に、前記出力部における前記出力を抑制する抑制部とを含むことを特徴とする。

【００２０】

また、前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、前記伝送手段は、前記フラグ情報を読み出し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記プログラム情報記憶手段から前記プログラム情報を読み出し、読み出したプログラム情報を出力し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていることを示す場合に、前記プログラム情報記憶手段から前記プログラム情報を読み出し、読み出したプログラム情報を前記鍵情報で暗号化し、暗号化されたプログラム情報を出力することを特徴とする。

【００２１】

前記マイクロプロセッサは、更に、キャッシュメモリを備え、前記プログラム

情報記憶手段は、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、前記実行手段は、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成した前記プログラム、データ又はプログラム及びデータを前記キャッシュメモリに書き込み、前記実行手段の実行速度に応じて前記キャッシュメモリから前記プログラム、データ又はプログラム及びデーを読み出し、読み出したプログラム、データ又はプログラム及びデータに従って動作し、前記伝送手段は、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を伝送することを特徴とする。

【００２２】

また、本発明は、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするホストコンピュータである。前記ホストコンピュータは、利用者から鍵情報の入力を受け付ける受付手段と、前記鍵情報を、内部に記憶すると共に前記マイクロプロセッサへ送出する送出手段と、記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備えることを特徴とする。

【００２３】

ここで、前記伝送手段は、前記マイクロプロセッサから、前記鍵情報を用いて暗号化されたプログラム情報を受け取るプログラム情報受取部と、前記暗号化されたプログラム情報に、記憶している前記鍵情報を用いて復号する復号部と、前記復号部が復号したプログラム情報を表示する表示部とを備えることを特徴とする。

【００２４】

ここで、前記伝送手段は、更に、利用者から、プログラム、データ又はプログラム及びデータを示すプログラム情報の入力を受け付けるプログラム情報入力部と、受け付けた前記プログラム情報に、記憶している前記鍵情報を用いて暗号化する暗号部と、前記暗号部が暗号化したプログラム情報を前記マイクロプロセッ

サへ出力する出力部とを備えることを特徴とする。

【００２５】

前記ホストコンピュータは、更に、ソースプログラムを記憶している記憶手段と、前記ソースプログラムを変換してプログラムを示すプログラム情報を生成する変換手段と、前記プログラム情報に、前記鍵情報を用いて暗号化する暗号化手段とを備え、前記伝送手段は、前記暗号化手段が暗号化したプログラム情報を前記マイクロプロセッサへ伝送することを特徴とする。

【００２６】

ここで、前記伝送手段は、さらに、鍵情報に係る情報で、前記マイクロプロセッサとの間の前記暗号化されたプログラム情報の伝送の停止を示す停止条件を記憶している停止条件記憶部と、前記入力手段が受け付けた前記鍵情報が、前記停止条件を満たす場合に、前記マイクロプロセッサに対して、前記暗号化されたプログラム情報の出力を抑制することを示す要求を出力する抑制要求出力部とを含むことを特徴とする。

【００２７】

また、本発明は、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと接続されたリードライト装置である。前記リードライト装置は、利用者から鍵情報の入力を受け付ける受付手段と、前記鍵情報を内部に記憶すると共に前記マイクロプロセッサへ送出する送出手段と、記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する伝送手段とを備えることを特徴とする。

【００２８】

【発明の実施の形態】

１．第１の実施の形態

本発明に係る第1の実施の形態として、デバッグシステム１について図面を参照して説明する。

＜構成＞

ここでは、デバッグシステム１の構成について説明する。デバッグシステム１は、マイクロプロセッサ１０、デバッグユニット１１、ホストＰＣ１２及び外部

メモリ１３から構成される。

【００２９】

マイクロプロセッサ１０と外部メモリ１３とは、ユーザが開発するＩＣカードの基板上に搭載されており、外部バスを介して互いに接続されている。また、デバッグユニット１１は、ケーブルを介してマイクロプロセッサ１０及びホストＰＣ１２と接続されている。ここで、外部メモリ１３には、命令及びデータから成るコンピュータプログラムが記憶されており、当該コンピュータプログラムは、マイクロプロセッサ１０により実行される。

【００３０】

以下では、マイクロプロセッサ１０及びホストＰＣ１２について詳しく説明する。

（マイクロプロセッサ１０）

図１は、マイクロプロセッサ１０の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ１０は、命令メモリ１０１、命令実行ユニット１０２、データメモリ１０３、データ処理ユニット１０４、不揮発性メモリ１０５、暗号化回路１０６、デバッグインターフェース１０７及びバスコントローラ１０８から構成される。

【００３１】

命令メモリ１０１は、具体的にはＲＡＭ（Random Access Memory）及びＲＯＭ（Read Only Memory）であって命令を記憶している。命令メモリ１０１は、バスを介して命令実行ユニット１０２と接続されている。更に、命令メモリ１０１は、バスを介して暗号化回路１０６と接続されており、デバッグユニット１１を介して接続されたホストＰＣ１２上で動作するデバッガの要求を受けて、記憶している命令を暗号化回路１０６へ出力する。また、命令メモリ１０１は、暗号化回路１０６から出力される命令を受け取り記憶する。

【００３２】

命令実行ユニット１０２は、バスを介して命令メモリ１０１と接続されており、命令メモリ１０１が記憶している命令を読み出し、解釈し、実行する。更に、命令実行ユニット１０２は、バスコントローラ１０８及び外部バスを介して外部

メモリ１３と接続されており、外部メモリ１３が記憶している命令を、バスコントローラ１０８を介して読み出し、解釈し、実行する。

【００３３】

データメモリ１０３は、具体的にはＲＯＭ又はＲＡＭであってデータを記憶している。データメモリ１０３は、バスを介してデータ処理ユニット１０４に接続されており、データ処理ユニット１０４からの要求を受けて、データ処理ユニット１０４へデータを出力する。データメモリ１０３は、データ処理ユニット１０４が出力する演算結果を受け取り記憶する。更に、データメモリ１０３は、バスを介して暗号化回路１０６と接続されており、デバッグユニット１１を介して接続されたホストＰＣ１２上で動作するデバッガの要求を受けて、記憶しているデータを暗号化回路１０６へ出力する。また、データメモリ１０３は、暗号化回路１０６から出力されるデータを受け取り記憶する。

【００３４】

データ処理ユニット１０４は、バスを介してデータメモリ１０３と接続されており、データメモリ１０３からデータを読み出し、読み出したデータに演算処理を施し、演算結果をデータメモリ１０３に書き込む。更に、データ処理ユニット１０４は、バス及びバスコントローラ１０８を介して外部メモリ１３と接続されており、外部メモリ１３が記憶しているデータを、バスコントローラ１０８を介して読み出し、読み出したデータに演算処理を施し、演算結果を外部メモリ１３に書き込む。

【００３５】

不揮発性メモリ１０５は、キーコードを記憶する領域と判定フラグを記憶する領域とを備え、キーコードと判定フラグとが書き込まれると、それらを所定の領域に記憶する。キーコードは、暗号化回路１０６による命令の暗号化及びデータの暗号化に用いられる暗号鍵であって、一度だけ書き込みが可能であり、読み出し及び書き換えが出来ない。判定フラグは、キーコードが不揮発性メモリ１０５に書き込み済みか否かを判定するために用いるフラグであって、キーコードが不揮発性メモリ１０５に書き込まれると、判定フラグが不揮発性メモリ１０５に書き込まれる。また、判定フラグは一度だけ書き込みが可能であり、書き換えが出

来ない。

【００３６】

暗号化回路１０６は、命令メモリ１０１に記憶されている命令をデバッグインターフェース１０７及びデバッグユニット１１を介してホストＰＣ１２が読み出すとき、また、データメモリ１０３に記憶されているデータをデバッグインターフェース１０７及びデバッグユニット１１を介してホストＰＣ１２が読み出すときに命令及びデータを暗号化するための回路である。暗号化回路１０６は、不揮発性メモリ１０５が記憶しているキーコードを暗号鍵として用いて命令メモリ１０１に記憶されている命令及びデータメモリに記憶されているデータに、暗号アルゴリズムE_1を施し暗号化命令及び暗号化データを生成する。ここで暗号アルゴリズムE_1は、例えばＤＥＳ（Data Encryption Standard）である。暗号化回路１０６は、生成した暗号化命令及び暗号化データをデバッグインターフェース１０７及びデバッグユニット１１を介してホストＰＣ１２へ出力する。

【００３７】

デバッグインターフェース１０７は、デバッグ端子を含むインターフェースであって、暗号化回路１０６とデバッグユニット１１、及び、不揮発性メモリ１０５とデバッグユニット１１を接続する。

更に、デバッグインターフェース１０７は、デバッグユニット１１を介してホストＰＣ１２から「命令表示」を示す信号を受け取ると、命令メモリ１０１から命令を抽出し、抽出した命令を暗号化回路１０６へ出力する。また、「データ表示」を示す信号を受け取ると、データメモリ１０３からデータを抽出し、抽出したデータを暗号化回路１０６へ出力する。また、デバッグインターフェース１０７は、デバッグユニット１１を介してホストＰＣ１２から命令を受け取ると、受け取った命令を、暗号化回路１０６を介して命令メモリ１０１へ書き込む。このとき、デバッグインターフェース１０７は、暗号化回路１０６に対して命令に暗号化処理を施さずに命令メモリ１０１へ書き込むことを指示する。データを受け取ると、受け取ったデータを、暗号化回路１０６を介してデータメモリ１０３へ書き込む。このとき、デバッグインターフェース１０７は、暗号化回路１０６に対してデータに暗号化処理を施さずにデータメモリ１０３へ書き込むことを指示

する。暗号化回路１０６はデータに対して暗号化処理を行わずに、データメモリ１０３へデータを書き込む。

【００３８】

バスコントローラ１０８は、マイクロプロセッサ１０の外部に設けられた外部メモリ１３と命令実行ユニット１０２、及び外部メモリ１３とデータ処理ユニット１０４との間で情報の受け渡しをする。

（ホストＰＣ１２）

ホストＰＣ１２は、マイクロプロセッサ１０に対応するデバッガが動作するコンピュータシステムであって、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるパーソナルコンピュータである。前記ハードディスクユニットには、デバッガを含む各種のコンピュータプログラムが記憶されている。

【００３９】

図２は、ホストＰＣ１２の機能を示す機能ブロック図である。同図に示す様に、ホストＰＣ１２は、表示部１２１とデバッグ部１２２とを備える。デバッグ部１２２は、前記ハードディスクユニットに記憶されているデバッガが前記マイクロプロセッサにより実行されるときの動作を機能的に示すものであり、デバッグ部１２２は、キーコード入力部１２３、コマンド入力部１２４、復号部１２５及び命令・データ入力部１２６を含む。

【００４０】

表示部１２１は、ディスプレイユニットを含み、デバッグ部１２２が出力する画面データをディスプレイに表示する。また、表示部１２１は、キーコードの入力を受け付けるための画面がディスプレイに表示されている状態において、キーコード入力部１２３が受け付けた内容を前記画面上に表示する。同様に、表示部１２１は、コマンドの入力を受け付けるための画面がディスプレイに表示されている状態において、コマンド入力部１２４が受け付けた内容を前記画面上に表示する。同様に、表示部１２１は、命令の入力を受け付けるための画面がディスプレイに表示されている状態において、命令・データ入力部１２６が受け付けた内容を前記画面上に表示する。同様に、データの入力を受け付けるための画面がデ

ィスプレイに表示されている状態において、命令・データ入力部１２６が受け付けた内容を前記画面上に表示する。

【００４１】

キーコード入力部１２３は、キーコードの入力を受け付けるための画面の生成に用いる画面情報を表示部１２１へ出力する。キーコード入力部１２３は、表示部１２１にキーコードの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したキーコードの入力を受け付ける。キーコード入力部１２３は、キーコードを受け付けると、受け付けたキーコードを記憶する。更に、キーコード入力部１２３は、デバッグユニット１１及びマイクロプロセッサ１０のデバッグインターフェース１０７を介して、不揮発性メモリ１０５から判定フラグを読み、不揮発性メモリ１０５にキーコードが書き込み済みか否か判断する。書き込み済みでない場合、キーコード入力部１２３は、キーコードを、デバッグユニット１１及びデバッグインターフェース１０７を介して不揮発性メモリ１０５に送出する。キーコード入力部１２３は、デバッグ部１２２の動作が終了すると、記憶したキーコードを破棄する。

【００４２】

コマンド入力部１２４は、コマンドの入力を受け付けるための画面の生成に用いる画面情報を表示部１２１へ出力する。コマンド入力部１２４は、表示部１２１にコマンドの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したコマンドの入力を受け付ける。更に、コマンド入力部１２４は、受け付けたコマンドを判断する。コマンドが「命令表示」であれは、コマンド入力部１２４は、「命令表示」を示す信号をデバッグユニット１１を介してデバッグインターフェース１０７へ送出する。コマンドが「命令書込み」であれば、コマンドに対応する信号を命令・データ入力部１２６へ出力する。コマンドが「データ表示」であれば、コマンド入力部１２４は、「データ表示」を示す信号をデバッグユニット１１を介してデバッグインターフェース１０７へ送出する。コマンドが「データ書込み」であれば、コマンド入力部１２４は、コマンドに対応する信号を命令・データ入力部１２６へ出力する。コマンドが「終了」であれば、ホストＰＣ１２のマイクロプロセッサは処理

を終了する。

【００４３】

復号部１２５は、デバッグユニット１１及びデバッグインターフェース１０７を介して、暗号化回路１０６から、暗号化回路１０６により暗号化された暗号化命令を受け取る。また、復号部１２５は、キーコード入力部１２３が記憶しているキーコードを読み出す。更に、復号部１２５は、読み出したキーコードを復号鍵として用い、受け取った暗号化命令に復号アルゴリズムD_1を施して、復号化命令を生成する。ここで、復号アルゴリズムD_1は、暗号アルゴリズムE_1により生成された暗号文を復号するアルゴリズムである。復号部１２５は、生成した復号化命令を表示部１２１へ出力する。同様にして、復号部１２５は、デバッグユニット１１及びデバッグインターフェース１０７を介して、暗号化回路１０６から、暗号化回路１０６により暗号化された暗号化データを受け取る。また、復号部１２５は、キーコード入力部１２３が記憶しているキーコードを読み出す。更に、復号部１２５は、読み出したキーコードを復号鍵として用い、受け取った暗号化データに復号アルゴリズムD_1を施して、復号化データを生成する。ここで、復号アルゴリズムD_1は、暗号アルゴリズムE_1により生成された暗号文を復号するアルゴリズムである。復号部１２５は、生成した復号化データを表示部１２１へ出力する。

【００４４】

不揮発性メモリ１０５が記憶しているキーコードと、キーコード入力部１２３が受け付けるキーコードが同じであれば、ホストＰＣ１２は、マイクロプロセッサ１０から取得した暗号化命令、及び暗号化データを正しく復号することができる。

命令・データ入力部１２６は、コマンド入力部１２４から、「命令書込み」を示す信号を受け取ると、命令の入力を受け付けるための画面の生成に用いる画面情報を表示部１２１へ出力する。命令・データ入力部１２６は、表示部１２１に、命令の入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボードを介した命令の入力を受け付ける。命令・データ入力部１２６は、入力を受け付けた命令をデバッグユニット１１を介してデバッグイン

ターフェース１０７へ送出する。命令・データ入力部１２６は、コマンド入力部１２４から、「データ書込み」を示す信号を受け取ると、データの入力を受け付けるための画面の生成に用いる画面情報を表示部１２１へ出力する。命令・データ入力部１２６は、表示部１２１に、データの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボードを介したデータの入力を受け付ける。命令・データ入力部１２６は、入力を受け付けたデータを、デバッグユニット１１を介してデバッグインターフェース１０７へ送出する。

【００４５】

＜動作＞

ここでは、図３及び図４に示すフローチャートを用いて、デバッグシステム１の動作について説明する。

ホストＰＣ１２のデバッグ部が起動し、キーコード入力部１２３が、ユーザからキーコードの入力を受け付け（ステップＳ１０１）、受け付けたキーコードを記憶する（ステップＳ１０２）。キーコード入力部１２３は、デバッグユニット１１を介して、マイクロプロセッサ１０の不揮発性メモリ１０５から、判定フラグを取得し、取得した判定フラグの状態を読み、不揮発性メモリ１０５にキーコードが書き込み済みか否かを判断する（ステップＳ１０３）。キーコードが書き込み済みでない場合（ステップＳ１０４でＮＯ）、キーコード入力部１２３は、先ほど記憶したキーコードを、デバッグユニット１１及びデバッグインターフェース１０７を介して不揮発性メモリ１０５に書き込む（ステップＳ１０５）。さらに、キーコード入力部１２３は、キーコードが書き込み済みであることを示す判定フラグを不揮発性メモリ１０５に書き込む（ステップＳ１０６）。

【００４６】

次に、ホストＰＣ１２のコマンド入力部１２４が、ユーザからコマンドの入力を受け付ける（ステップＳ１０７）。ここで、コマンドの種類は、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であり、これらの内の何れか一つがユーザにより選択される。コマンド入力部１２４は、選択されたコマンドを判断する（ステップＳ１０８）。

【００４７】

コマンドが「命令表示」であれば（ステップＳ１０８で「命令表示」）、コマンド入力部１２４は、デバッグインターフェース１０７へ信号を送出し、デバッグインターフェース１０７は、命令メモリ１０１に格納されている命令を抽出し（ステップＳ１０９）、暗号化回路１０６に出力する。暗号化回路１０６は、命令を受け取り、不揮発性メモリ１０５に保持されているキーコードを用いて、受け取った命令を暗号化する（ステップＳ１１０）。暗号化回路１０６は、暗号化した命令を、デバッグインターフェース１０７及びデバッグユニット１１を介してホストＰＣ１２に出力する（ステップＳ１１１）。ホストＰＣ１２の復号部１２５は、暗号化された命令を受け取り、ステップＳ１０２において記憶したキーコードを用いて受け取った命令を復号する（ステップＳ１１２）。復号部１２５は、復号した命令を表示部１２１へ出力し、表示部１２１は、命令を受け取りディスプレイに表示する（ステップＳ１１３）。このとき、ステップＳ１０１において入力されたキーコードが、不揮発性メモリ１０５に保持されているキーコードと同じであれば、命令は正しく表示され、キーコードが同じでなければ、命令は正しく表示されない。その後、ステップＳ１０７に戻り処理を続ける。

【００４８】

コマンドが「命令書込み」であれば（ステップＳ１０８で「命令書込み」）、ホストＰＣ１２の命令・データ入力部１２６は、ユーザから命令の入力を受け付ける（ステップＳ１２１）。命令・データ入力部１２６は、受け付けた命令をデバッグユニット１１を介してデバッグインターフェース１０７へ送出し、デバッグインターフェース１０７は、命令を暗号化回路１０６へ出力する（ステップＳ１２２）。暗号化回路１０６は、デバッグインターフェース１０７から命令を受け取り、受け取った命令を命令メモリ１０１に書き込む（ステップＳ１２３）。このとき、暗号化回路１０６は、命令に暗号化処理を施さず、命令を命令メモリ１０１に書き込むだけである。その後、ステップＳ１０７に戻り処理を続ける。

【００４９】

コマンドが「データ表示」であれば（ステップＳ１０８で「データ表示」）、コマンド入力部１２４は、デバッグインターフェース１０７へ信号を送出し、デバッグインターフェース１０７は、データメモリ１０３に格納されているデータ

を抽出し（ステップＳ１３１）、暗号化回路１０６に出力する。暗号化回路１０６は、データを受け取り、不揮発性メモリ１０５に保持されているキーコードを用いて、受け取ったデータを暗号化する（ステップＳ１３２）。暗号化回路１０６は、暗号化したデータを、デバッグインターフェース１０７及びデバッグユニット１１を介してホストＰＣ１２に出力する（ステップＳ１３３）。ホストＰＣ１２の復号部１２５は、暗号化されたデータを受け取り、ステップＳ１０２において記憶したキーコードを用いて受け取ったデータを復号する（ステップＳ１３４）。復号部１２５は、復号したデータを表示部１２１へ出力し、表示部１２１は、データを受け取りディスプレイに表示する（ステップＳ１３５）。このとき、ステップＳ１０１において入力されたキーコードが、不揮発性メモリ１０５に保持されているキーコードと同じであれば、データは正しく表示され、キーコードが同じでなければ、データは正しく表示されない。その後、ステップＳ１０７に戻り処理を続ける。

【００５０】

コマンドが「データ書込み」であれば（ステップＳ１０８で「データ書込み」）、ホストＰＣ１２の命令・データ入力部１２６は、ユーザからデータの入力を受け付ける（ステップＳ１４１）。命令・データ入力部１２６は、受け付けたデータを、デバッグユニット１１を介してデバッグインターフェース１０７へ送出し、デバッグインターフェース１０７は、データを暗号化回路１０６へ出力する（ステップＳ１４２）。暗号化回路１０６は、デバッグインターフェース１０７からデータを受け取り、受け取ったデータをデータメモリ１０３に書き込む（ステップＳ１４３）。このとき、暗号化回路１０６は、データに暗号化処理を施さず、データをデータメモリ１０３に書き込むだけである。その後、ステップＳ１０７に戻り処理を続ける。

【００５１】

コマンドが「終了」であれば（ステップＳ１０８で「終了」）、処理を終了する。

２．第２の実施の形態

本発明に掛かる第２の実施の形態として、デバッグシステム２について図面を

参照して説明する。

【００５２】

＜構成＞

ここでは、デバッグシステム２の構成について説明する。デバッグシステム２は、マイクロプロセッサ２０、デバッグユニット２１及びホストＰＣ２２から構成される。マイクロプロセッサ２０は、ユーザが開発するＩＣカードの基板上に搭載されており、デバッグユニット２１は、ケーブルを介してマイクロプロセッサ２０及びホストＰＣ２２と接続されている。

【００５３】

以下では、マイクロプロセッサ２０及びホストＰＣ２２について詳しく説明する。

（マイクロプロセッサ２０）

図５は、マイクロプロセッサ２０の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ２０は、命令メモリ２０１、命令実行ユニット２０２、データメモリ２０３、データ処理ユニット２０４、不揮発性メモリ２０５、復号化回路２０６及びデバッグインターフェース２０７から構成される。

【００５４】

命令メモリ２０１は、具体的にはＲＡＭ及びＲＯＭであって、暗号化命令を記憶している。命令メモリ２０１が記憶している暗号化命令は、予め、ホストＰＣ２２のコンパイル部２２４が、命令に暗号アルゴリズムE_2を施して生成した暗号化命令である。ホストＰＣ２２のコンパイル部２２４については後述する。命令メモリ２０１は、バスを介して復号化回路２０６と接続されている。更に、命令メモリ２０１は、バスを介してデバッグインターフェース２０７と接続されており、デバッグユニット２１を介して接続されたホストＰＣ２２上で動作するデバッガの要求を受けて、記憶している暗号化命令をデバッグインターフェース２０７及びデバッグユニット２１を介してホストＰＣ２２へ出力する。また、命令メモリ２０１は、デバッグインターフェース２０７から出力される暗号化命令を受け取り記憶する。

【００５５】

命令実行ユニット２０２は、バスを介して復号化回路２０６と接続されており、復号化回路２０６から命令を受け取り、受け取った命令を解釈し、実行する。

データメモリ２０３は、具体的にはＲＯＭ又はＲＡＭであってデータを記憶している。データメモリ２０３は、バスを介してデータ処理ユニット２０４に接続されており、データ処理ユニット２０４からの要求を受けて、データ処理ユニット２０４へデータを出力する。データメモリ２０３は、データ処理ユニット２０４が出力する演算結果を受け取り記憶する。更に、データメモリ２０３は、バスを介してデバッグインターフェース２０７と接続されており、デバッグユニット２１を介して接続されたホストＰＣ２２上で動作するデバッガの要求を受けて、記憶しているデータをデバッグインターフェース２０７へ出力する。また、データメモリ２０３は、デバッグインターフェース２０７から出力されるデータを受け取り記憶する。

【００５６】

データ処理ユニット２０４は、バスを介してデータメモリ２０３と接続されており、データメモリ２０３からデータを読み出し、読み出したデータに演算処理を施し、演算結果をデータメモリ２０３に書き込む。

不揮発性メモリ２０５は、キーコードを記憶する領域と判定フラグを記憶する領域とを備え、キーコードと判定フラグとが書き込まれると、それらを所定の領域に記憶する。キーコードは、復号化回路２０６による命令の復号化に用いられる復号鍵であって、一度だけ書き込みが可能であり、読み出し及び書き換えが出来ない。判定フラグは、キーコードが不揮発性メモリ２０５に書き込み済みか否かを判定するために用いるフラグであって、キーコードが不揮発性メモリ２０５に書き込まれると、判定フラグが不揮発性メモリ２０５に書き込まれる。また、判定フラグは一度だけ書き込みが可能であり、書き換えが出来ない。

【００５７】

復号化回路２０６は、命令メモリ２０１に記憶されている暗号化命令を命令実行ユニット２０２が読み出すときに、暗号化命令を復号化するための回路である。復号化回路２０６は、不揮発性メモリ２０５が記憶しているキーコードを復号鍵として用いて命令メモリ２０１に記憶されている暗号化命令に復号アルゴリズ

ムD$_2$を施し命令を生成する。ここで、復号アルゴリズムD$_2$は、暗号アルゴリズムE$_2$により生成された暗号文を復号するアルゴリズムである。復号化回路２０６は、生成した命令を命令実行ユニット２０２へ出力する。

【００５８】

デバッグインターフェース２０７は、デバッグユニット２１との接続に用いられるデバッグ端子を含むインターフェースである。デバッグインターフェース２０７は、デバッグ端子を含み、命令メモリ２０１とデバッグユニット２１、データメモリ２０３とデバッグユニット２１及び不揮発性メモリ２０５とデバッグユニット２１とを接続するインターフェースである。

【００５９】

デバッグインターフェース２０７は、デバッグユニット２１を介してホストＰＣ２２から「命令表示」を示す信号を受け取ると、命令メモリ２０１から命令を抽出する。また、「データ表示」を示す信号を受け取ると、データメモリ１０３からデータを抽出し、抽出したデータをデバッグユニット２１へ出力する。また、デバッグインターフェース１０７は、デバッグユニット２１を介してホストＰＣ２２から暗号化命令を受け取ると、受け取った暗号化命令を、命令メモリ２０１へ書き込む。データを受け取ると、受け取ったデータを、データメモリ２０３へ書き込む。

【００６０】

（ホストＰＣ２２）

ホストＰＣ２２は、マイクロプロセッサ２０に対応するデバッガ及びコンパイラが動作するコンピュータシステムであり、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード及びマウスなどから構成されるパーソナルコンピュータである。前記ハードディスクユニットには、デバッガ及びコンパイラを含む各種のコンピュータプログラムが記憶されている。

【００６１】

図６は、ホストＰＣ２２の構成を示すブロック図である。同図に示す様に、ホストＰＣ２２は、表示部２２１、デバッグ部２２２、ソースファイル２２３、コ

ンパイル部２２４及び暗号化オブジェクトファイル２３５を備える。デバッグ部２２２は、前記ハードディスクユニットに記憶されているデバッガが前記マイクロプロセッサにより実行されるときの動作を機能的に示すものであり、デバッグ部２２２は、キーコード入力部２２５、コマンド入力部２２６、復号部２２７、命令・データ入力部２２８及び暗号部２２９を含む。

【００６２】

また、コンパイル部２２４は、前記ハードディスクユニットに記憶されているコンパイラが前記マイクロプロセッサにより実行されるときの動作を機能的に示すものであり、コンパイル部２２４は、コンパイル、アセンブル、リンク処理部２３１、オブジェクトファイル２３２、キーコード入力部２３３及び暗号部２３４を含む。

【００６３】

表示部２２１は、ディスプレイユニットを含み、デバッグ部２２２が出力する画面データをディスプレイに表示する。また、表示部２２１は、キーコードの入力を受け付けるための画面がディスプレイに表示されている状態において、キーコード入力部２２５が受け付けた内容を前記画面上に表示する。同様に、表示部２２１は、コマンドの入力を受け付けるための画面がディスプレイに表示されている状態において、コマンド入力部２２６が受け付けた内容を前記画面上に表示する。同様に、表示部２２１は、命令の入力を受け付けるための画面がディスプレイに表示されている状態において、命令・データ入力部２２８が受け付けた内容を前記画面上に表示する。同様に、データの入力を受け付けるための画面がディスプレイに表示されている状態において、命令・データ入力部２２８が受け付けた内容を前記画面上に表示する。

【００６４】

キーコード入力部２２５は、キーコードの入力を受け付けるための画面の生成に用いる画面情報を表示部２２１へ出力する。キーコード入力部２２５は、表示部２２１にキーコードの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したキーコードの入力を受け付け、受け付けたキーコードを記憶する。更に、キーコード入力部２２５は

、デバッグユニット２１及びマイクロプロセッサ２０のデバッグインターフェース２０７を介して、不揮発性メモリ２０５から判定フラグを読み、不揮発性メモリ２０５にキーコードが書き込み済みか否か判断する。書き込み済みでない場合、キーコード入力部２２５は、キーコードを、デバッグユニット２１及びデバッグインターフェース２０７を介して不揮発性メモリ２０５に送出する。キーコード入力部２２５は、デバッグ部２２２の動作が終了すると、記憶したキーコードを破棄する。

【００６５】

コマンド入力部２２６は、コマンドの入力を受け付けるための画面の生成に用いる画面情報を表示部２２１へ出力する。コマンド入力部２２６は、表示部２２１にコマンドの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したコマンドの入力を受け付ける。更に、コマンド入力部２２６は、受け付けたコマンドを判断する。コマンドが「命令表示」であれは、コマンド入力部２２６は、「命令表示」を示す信号を、デバッグユニット２１を介してデバッグインターフェース２０７へ送出する。コマンドが「命令書込み」であれば、コマンドに対応する信号を命令・データ入力部２２８へ出力する。コマンドが「データ表示」であれば、コマンド入力部２２６は、「データ表示」を示す信号を、デバッグユニット２１を介してデバッグインターフェース２０７へ送出する。コマンドが「データ書込み」であれば、コマンド入力部２２６は、コマンドに対応する信号を命令・データ入力部２２８へ出力する。コマンドが「終了」であれば、処理を終了する。

【００６６】

復号部２２７は、デバッグユニット２１及びデバッグインターフェース２０７を介して、命令メモリ２０１から暗号化命令を受け取る。また、復号部２２７は、キーコード入力部２２５が記憶しているキーコードを読み出す。更に、復号部２２７は、読み出したキーコードを復号鍵として用い、受け取った暗号化命令に復号アルゴリズムD_2を施して、復号化命令を生成する。復号部２２７は、生成した復号化命令を表示部２２１へ出力する。

【００６７】

不揮発性メモリ２０５が記憶しているキーコードと、キーコード入力部２２５が受け付けるキーコードが同じであれば、ホストＰＣ２２は、マイクロプロセッサ２０から取得した暗号化命令を正しく復号することができる。

命令・データ入力部２２８は、コマンド入力部２２６から、「命令書込み」を示す信号を受け取ると、命令の入力を受け付けるための画面の生成に用いる画面情報を表示部２２１へ出力する。命令・データ入力部２２８は、表示部２２１に、命令の入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボードを介した命令の入力を受け付ける。命令・データ入力部２２８は、入力を受け付けた命令を暗号部２２９へ出力する。命令・データ入力部２２８は、コマンド入力部２２６から、「データ書込み」を示す信号を受け取ると、データの入力を受け付けるための画面の生成に用いる画面情報を表示部２２１へ出力する。命令・データ入力部２２８は、表示部２２１に、データの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボードを介したデータの入力を受け付ける。命令・データ入力部２２８は、入力を受け付けたデータをデバッグユニット２１を介してデバッグインターフェース２０７へ送出する。

【００６８】

暗号部２２９は、命令・データ入力部２２８から命令を受け取り、キーコード入力部２２５が記憶しているキーコードを読み出す。更に、暗号部２２９は、読み出したキーコードを暗号鍵として用い、受け取った命令に暗号アルゴリズムE_2を施して、暗号化命令を生成する。暗号部２２９は、生成した暗号化命令をデバッグユニット２１を介してデバッグインターフェース２０７へ送出する。

【００６９】

コンパイル、アセンブル、リンク処理部２３１は、外部記憶装置からソースファイル２２３を読み込み、ソースファイル２２３にコンパイル、アセンブル及びリンク処理を施してオブジェクトファイル２３２を生成する。キーコード入力部２３３は、キーボード及びマウスを介したキーコードの入力を受け付ける。キーコード入力部２３３は、受け付けたキーコードを記憶する。暗号部２３４は、キーコード入力部２３３に記憶されているキーコードを暗号鍵として用いて、オブ

ジェクトファイル２３２に暗号アルゴリズムE_2を施して暗号化オブジェクトファイル２３５を生成する。コンパイル部２２４は、生成した暗号化オブジェクトファイル２３５を外部記憶装置へ書き込む。

【００７０】

＜動作＞

ここでは、図３及び図７に示すフローチャートを用いて、デバッグシステム２の動作について説明する。

図３のステップＳ１０１からステップＳ１０８まで、デバッグシステム２の動作は、前述したデバッグシステム１の動作と同様であるため説明を省略し、図７から説明する。

【００７１】

コマンドが「命令表示」であれば（ステップＳ１０８で「命令表示」）、デバッグ部２２２は、コマンドに対応する信号をデバッグユニット２１を介してデバッグインターフェース２０７へ送出し、デバッグインターフェース２０７は、命令メモリ２０１に格納されている暗号化命令を読み出して、デバッグユニット２１を介して読み出した暗号化命令を復号部２２７へ渡す（ステップＳ２０１）。復号部２２７は、暗号化命令を受け取り、キーコード入力部２２５が受け付けたキーコードを用いて、受け取った暗号化命令を復号する（ステップＳ２０２）。復号部２２７は、復号した命令を表示部２２１へ出力し、表示部２２１は、命令を受け取りディスプレイに表示する（ステップＳ２０３）。その後、図３のステップＳ１０７に戻り処理を続ける。

【００７２】

コマンドが「命令書込み」であれば（ステップＳ１０８で「命令書込み」）、ホストＰＣ２２の命令・データ入力部２２８は、ユーザから命令の入力を受け付ける（ステップＳ２０６）。命令・データ入力部２２８は、受け付けた命令を暗号部２２９へ渡す。暗号部２２９は、キーコード入力部２２５が記憶しているキーコードを読み出し、読み出したキーコードを暗号鍵として用いて、命令を暗号化する（ステップＳ２０７）。暗号部２２９は生成した暗号化命令をデバッグユニット２１を介してデバッグインターフェース２０７へ送出する（ステップＳ２

０８）。デバッグインターフェース２０７は、暗号化命令を受け取り、受け取った暗号化命令を命令メモリ２０１に格納する（ステップＳ２０９）。その後、ステップＳ１０７に戻り処理を続ける。

【００７３】

コマンドが「データ表示」であれば（ステップＳ１０８で「データ表示」）、ホストＰＣ２２のデバッグ部２２２は、コマンドに対応する信号をデバッグユニット２１を介してデバッグインターフェース２０７へ送出し、デバッグインターフェース２０７は、データメモリ２０３に格納されているデータを読み出して、デバッグユニット２１を介して表示部２２１に出力する（ステップＳ２２１）。表示部２２１は、データを受け取り、ディスプレイに表示する（ステップＳ２２２）。その後、ステップＳ１０７に戻り処理を続ける。

【００７４】

コマンドが「データ書込み」であれば（ステップＳ１０８で「データ書込み」）、ホストＰＣ２２の命令・データ入力部２２８は、ユーザからデータの入力を受け付ける（ステップＳ２３１）。命令・データ入力部２２８は、受け付けたデータを、デバッグユニット２１を介してデバッグインターフェース２０７へ送出する（ステップＳ２３２）。デバッグインターフェース２０７は、データを受け取り、受け取ったデータをデータメモリ２０３に格納する（ステップＳ２３３）。その後、ステップＳ１０７に戻り処理を続ける。

【００７５】

コマンドが「終了」であれば（ステップＳ１０８で「終了」）、処理を終了する。

＜変形例１＞

デバッグシステム２の変形例として、デバッグシステム３について説明する。

（構成）

デバッグシステム３は、マイクロプロセッサ３０、デバッグユニット３１、ホストＰＣ３２及び外部メモリ３３から構成される。マイクロプロセッサ３０と外部メモリ３３とは、ユーザが開発するＩＣカードの基板上に搭載されており、外部バスを介して互いに接続されている。また、デバッグユニット３１は、ケーブ

ルを介してマイクロプロセッサ３０及びホストＰＣ３２と接続されている。ここで、外部メモリ３３には、暗号化命令及びデータが記憶されており、前記暗号化命令は、命令にマイクロプロセッサ３０の不揮発性メモリ３０５に格納されているキーコードと同一の暗号鍵を用い、暗号アルゴリズムE_2を施して生成したものである。前記暗号化命令は、マイクロプロセッサ３０により復号され、実行される。

【００７６】

デバッグシステム２との相違点は、外部メモリ３３がマイクロプロセッサ３０に接続されていることである。なお、ホストＰＣ３２の構成は図示していない。ホストＰＣ３２は、デバッグシステム２のホストＰＣ２２と同様の構成及び機能を有するため、ここでは説明を省略し、以下ではマイクロプロセッサ３０について、マイクロプロセッサ２０との相違点を中心に説明する。

【００７７】

図８は、マイクロプロセッサ３０の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ３０は、命令メモリ３０１、命令実行ユニット３０２、データメモリ３０３、データ処理ユニット３０４、不揮発性メモリ３０５、復号化回路３０６、デバッグインターフェース３０７及びバスコントローラ３０８から構成される。

【００７８】

命令メモリ３０１、データメモリ３０３、不揮発性メモリ３０５及びデバッグインターフェース３０７は、それぞれ、命令メモリ２０１、データメモリ２０３、不揮発性メモリ２０５、デバッグインターフェース２０７と同様の機能を有するため、説明を省略する。

命令実行ユニット３０２は、バスを介して復号化回路３０６と接続されており、復号化回路３０６から命令を受け取り、受け取った命令を解釈し、実行する。ここで、命令実行ユニット３０２が復号化回路３０６から受け取る命令は、命令メモリ３０１に格納されていた暗号化命令を復号化して生成した命令及び外部メモリ３３に格納されていた暗号化命令と復号化して生成した命令である。

【００７９】

データ処理ユニット３０４は、バスを介してデータメモリ３０３と接続されており、データメモリ３０３からデータを読み出し、読み出したデータに演算処理を施し、演算結果をデータメモリ３０３に書き込む。更に、データ処理ユニット３０４は、バス及びバスコントローラ３０８を介して外部メモリ３３と接続されており、外部メモリ３３が記憶しているデータを、バスコントローラ３０８を介して読み出し、読み出したデータに演算処理を施し、演算結果を外部メモリ３３に書き込む。

【００８０】

復号化回路３０６は、不揮発性メモリ３０５が記憶しているキーコードを復号鍵として用いて命令メモリ３０１に記憶されている暗号化命令に復号アルゴリズムD_2を施し復号化命令を生成する。更に、復号化回路３０６は、外部メモリ３３に記憶されている暗号化命令に復号アルゴリズムD_2を施し復号化命令を生成する。ここで、復号アルゴリズムD_2は、暗号アルゴリズムE_2により生成された暗号文を復号するアルゴリズムである。復号化回路３０６は、生成した復号化命令を命令実行ユニット２０２へ出力する。

【００８１】

バスコントローラ３０８は、マイクロプロセッサ３０の外部に設けられた外部メモリ３３と命令実行ユニット３０２、及び外部メモリ２３とデータ処理ユニット３０４との間で情報の受け渡しをする。

デバッグシステム３の動作は、図３及び図７に示したデバッグシステム２の動作と同様であるため説明を省略する。

【００８２】

＜変形例２＞

デバッグシステム２の変形例として、デバッグシステム４について説明する。

（構成）

デバッグシステム４は、マイクロプロセッサ４０、デバッグユニット４１及びホストＰＣ４２から構成される。マイクロプロセッサ４０は、ユーザが開発するＩＣカードの基板上に搭載されており、デバッグユニット４１は、ケーブルを介してマイクロプロセッサ１０及びホストＰＣ１２と接続されている。

【００８３】

デバッグシステム２との相違点は、マイクロプロセッサ４０は、データに暗号アルゴリズムE_2を施して生成した暗号化データを内部に保持しており、暗号化データを復号した後にデータ処理を行う。マイクロプロセッサ４０は、データ処理後の演算結果に暗号アルゴリズムE_2を施して暗号化データを生成し、生成した暗号化データを記憶する。以下ではマイクロプロセッサ４０について、マイクロプロセッサ２０との相違点を中心に説明する。

【００８４】

図９は、マイクロプロセッサ４０の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ３０は、命令メモリ４０１、命令実行ユニット４０２、データメモリ４０３、データ処理ユニット４０４、不揮発性メモリ４０５、復号化回路４０６、デバッグインターフェース４０７及び暗復号化回路４０８から構成される。

【００８５】

命令メモリ４０１、命令実行ユニット４０２及びデバッグインターフェース４０７は、それぞれ、命令メモリ２０１、命令実行ユニット２０２及びデバッグインターフェース２０７と同様の機能を有するため、説明を省略する。

データメモリ４０３は、具体的にはＲＯＭ又はＲＡＭであって、暗号化データを保持する。ここで、データメモリ４０３が保持している暗号化データは、データに、不揮発性メモリ４０５が保持しているキーコードと同一のデータを暗号鍵として用い、暗号アルゴリズムE_2を施して生成したものである。データメモリ４０３は、バスを介して暗復号化回路４０８と接続されており、データ処理ユニット４０４からの要求を受けて、暗号化データを暗復号化回路４０８へ出力する。データメモリ４０３は、暗復号化回路４０８が暗号化した演算結果を受け取り記憶する。更に、データメモリ４０３は、バスを介してデバッグインターフェース４０７と接続されており、デバッグユニット４１を介して接続されたホストＰＣ４２上で動作するデバッガの要求を受けて、記憶している暗号化データをデバッグインターフェース４０７へ出力する。また、データメモリ４０３は、デバッグインターフェース４０７から出力される暗号化データを受け取り記憶する。

【００８６】

データ処理ユニット４０４は、バスを介して暗復号化回路４０８と接続されており、暗復号化回路４０８からデータを受け取り、受け取ったデータに演算処理を施し、演算結果を暗復号化回路４０８に出力する。

復号化回路４０６は、バスを介して命令メモリ４０１及び不揮発性メモリ４０５に接続されており、命令メモリ４０１から暗号化命令を受け取り、更に、不揮発性メモリ４０５からキーコードを読み出す。復号化回路４０６は読み出したキーコードを復号鍵として用い、受け取った暗号化命令に復号アルゴリズムD_2を施し復号化命令を生成する。ここで、復号アルゴリズムD_2は、暗号アルゴリズムE_2により生成された暗号文を復号するアルゴリズムである。復号化回路４０６は、生成した復号化命令を命令実行ユニット４０２へ出力する。

【００８７】

暗復号化回路４０８は、暗号化回路と復号化回路とから構成される。暗復号化回路４０８は、データメモリ４０３から暗号化データの入力を受け付ける場合、復号化回路を用いてデータを生成し、生成したデータをデータ処理ユニット４０４へ出力する。暗復号化回路４０８は、データ処理ユニット４０４からデータの入力を受け付ける場合、暗号化回路を用いて暗号化データを生成し、生成した暗号化データをデータメモリ４０３へ出力する。

【００８８】

ホストＰＣ４２は、マイクロプロセッサ４０に対応したデバッガ及びコンパイラが動作するパーソナルコンピュータである。図１０に示す様に、ホストＰＣ４２は、表示部４２１、デバッグ部４２２、ソースファイル４２３及びコンパイル部４２４を備える。デバッグ部４２２は、ホストＰＣ４２上で動作するデバッガを機能的に示すもので、キーコード入力部４２５、コマンド入力部４２６、復号部４２７、命令・データ入力部４２８及び暗号部４２９を含む。コンパイル部４２４は、ホストＰＣ４２上で動作するコンパイラ、アセンブラ及びリンカを機能的に示すもので、コンパイル、アセンブル、リンク処理部４３１、オブジェクトファイル４３２、キーコード入力部４３３及び暗号部４３４を含む。ホストＰＣ４２は、ホストＰＣ２２と同様の機能を有するため、詳細な説明は省略する。

【００８９】

（動作）

ここでは、図３及び図１１に示すフローチャートを用いて、デバッグシステム４の動作について説明する。

図３のステップＳ１０１からステップＳ１０８まで、デバッグシステム４の動作は、前述したデバッグシステム１の動作と同様であるため説明を省略し、図１１から説明する。

【００９０】

コマンドが「命令表示」であれば（ステップＳ１０８で「命令表示」）、ホストＰＣ４２のデバッグ部４２２は、コマンドに対応する信号をデバッグユニット４１を介してデバッグインターフェース４０７へ送出し、デバッグインターフェース４０７は、命令メモリ４０１に格納されている暗号化命令を読み出して、デバッグユニット４１を介して復号部４２７へ渡す（ステップＳ４０１）。復号部４２７は、デバッグユニット４１を介してデバッグインターフェース４０７から暗号化命令を受け取り、キーコード入力部４２５が受け付けたキーコードを用いて、受け取った暗号化命令を復号する（ステップＳ４０２）。復号部４２７は、復号した命令を表示部４２１へ出力し、表示部４２１は、命令を受け取りディスプレイに表示する（ステップＳ４０３）。その後、図３のステップＳ１０７に戻り処理を続ける。

【００９１】

コマンドが「命令書込み」であれば（ステップＳ１０８で「命令書込み」）、ホストＰＣ４２の命令・データ入力部２２８は、ユーザから命令の入力を受け付ける（ステップＳ４１１）。命令・データ入力部４２８は、受け付けた命令を暗号部４２９へ出力する。暗号部４２９は、キーコード入力部４２５が記憶しているキーコードを読み出し、読み出したキーコードを暗号鍵として用いて、命令を暗号化する（ステップＳ４１２）。暗号部４２９は生成した暗号化命令をデバッグユニット４１を介してデバッグインターフェース４０７へ送出する（ステップＳ４１３）。デバッグインターフェース４０７は、暗号化命令を受け取り、受け取った暗号化命令を命令メモリ４０１に格納する（ステップＳ４１４）。その後

、ステップＳ１０７に戻り処理を続ける。

【００９２】

コマンドが「データ表示」であれば（ステップＳ１０８で「データ表示」）、ホストＰＣ４２のデバッグ部４２２は、コマンドに対応する信号をデバッグユニット４１を介してデバッグインターフェース４０７へ送出し、デバッグインターフェース４０７は、データメモリ４０３に格納されている暗号化データを読み出し、デバッグユニット４１を介して復号部４２７に渡す（ステップＳ４２１）。復号部４２７は、デバッグユニット４１を介してデバッグインターフェース４０７から暗号化データを受け取り、キーコード入力部４２５が受け付けたキーコードを用いて、受け取った暗号化データを復号する（ステップＳ４２２）。復号部４２７は、復号したデータを表示部４２１へ出力し、表示部４２１は、データを受け取りディスプレイに表示する（ステップＳ４２３）。その後、図３のステップＳ１０７に戻り処理を続ける。

【００９３】

コマンドが「データ書込み」であれば（ステップＳ１０８で「データ書込み」）、ホストＰＣ４２の命令・データ入力部４２８は、ユーザからデータの入力を受け付ける（ステップＳ４３１）。命令・データ入力部４２８は、受け付けたデータを暗号部４２９へ渡す。暗号部４２９は、キーコード入力部４２５が記憶しているキーコードを読み出し、読み出したキーコードを暗号鍵として用いて、データを暗号化する（ステップＳ４３２）。暗号部４２９は生成した暗号化データをデバッグユニット４１を介してデバッグインターフェース４０７へ送出する（ステップＳ４３３）。デバッグインターフェース４０７は、暗号化データを受け取り、受け取った暗号化データをデータメモリ４０３に格納する（ステップＳ４３４）。その後、ステップＳ１０７に戻り処理を続ける。

【００９４】

コマンドが「終了」であれば（ステップＳ１０８で「終了」）、処理を終了する。

＜変形例３＞

デバッグシステム２の変形例として、デバッグシステム５について説明する。

（構成）

デバッグシステム５は、図１２に示す様に、マイクロプロセッサ５０、メモリリードライト装置５１及びホストＰＣ５２から構成される。マイクロプロセッサ５０は、ユーザが開発するＩＣカードの基板上に搭載されている。メモリリードライト装置５１は、マイクロプロセッサ５０のメモリのプログラム及びデータの読み出し、及びマイクロプロセッサ５０のメモリにプログラム及びデータの書き込みを行う装置であって、マイクロプロセッサ５０及びホストＰＣ５２と、それぞれケーブルを介して接続されている。

【００９５】

マイクロプロセッサ５０は、命令メモリ５０１、命令実行ユニット５０２、データメモリ５０３、データ処理ユニット５０４、不揮発性メモリ５０５、復号化回路５０６及びデバッグインターフェース５０７から構成される。マイクロプロセッサ５０は、図５に示したマイクロプロセッサ２０と同様の構成を有するため、マイクロプロセッサ５０の構成を示すブロック図は示していない。マイクロプロセッサ５０の各構成要素は、それぞれ、マイクロプロセッサ２０の命令メモリ２０１、命令実行ユニット２０２、データメモリ２０３、データ処理ユニット２０４、不揮発性メモリ２０５、復号化回路２０６及びデバッグインターフェース２０７を同様の機能を有するため、ここでは説明を省略する。

【００９６】

ホストＰＣ５２は、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード及びマウスなどから構成されるパーソナルコンピュータである。前記ハードディスクユニットには、メモリリードライト装置制御プログラムを含む各種のコンピュータプログラムが記憶されている。

【００９７】

図１１は、ホストＰＣ５２の機能を示す機能ブロック図である。同図に示す様に、ホストＰＣ５２は、表示部５２１、メモリリードライト装置制御部５２２、ソースファイル５２３及びコンパイル部５２４を備える。メモリリードライト装置制御部５２２は、更に、キーコード入力部５２５、メモリ操作コマンド入力部

５２６、復号部５２７及び暗号部５２８を含む。

【００９８】

表示部５２１は、ディスプレイユニットを含み、メモリリードライト装置制御部５２２が出力する画面データをディスプレイに表示する。また、表示部５２１は、キーコードの入力を受け付けるための画面がディスプレイに表示されている状態において、キーコード入力部５２５が受け付けた内容を前記画面上に表示する。同様に、表示部５２１は、コマンドの入力を受け付けるための画面がディスプレイに表示されている状態において、メモリ操作コマンド入力部５２６が受け付けた内容を前記画面上に表示する。

【００９９】

キーコード入力部５２５は、具体的にはキーボード及びマウス等を含み、キーコードの入力を受け付けるための画面の生成に用いる画面情報を表示部５２１へ出力する。キーコード入力部５２５は、表示部５２１にキーコードの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したキーコードの入力を受け付ける。キーコード入力部５２５は、受け付けたキーコードを記憶する。更に、キーコード入力部５２５は、受け付けたキーコードを、メモリリードライト装置５１を介してデバッグインターフェース５０７へ送出する。キーコード入力部５２５は、メモリリードライト装置制御部５２２の動作が終了すると、記憶しているキーコードを破棄する。

【０１００】

メモリ操作コマンド入力部５２６は、具体的にはキーボード及びマウス等を含み、コマンドの入力を受け付けるための画面の生成に用いる画面情報を表示部５２１へ出力する。メモリ操作コマンド入力部５２６は、表示部５２１にコマンドの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したコマンドの入力を受け付ける。更に、メモリ操作コマンド入力部５２６は、受け付けたコマンドを判断する。

【０１０１】

コマンドが「メモリ読出し」であれは、メモリ操作コマンド入力部５２６は、コマンドに対応する信号を、メモリリードライト装置５１を介してデバッグイン

ターフェース５０７へ送出する。コマンドが「メモリ書込み」であれば、メモリ操作コマンド入力部５２６は、コンパイル部５２４にファイルを指定する信号を出力する。コマンドが「終了」であれば、マイクロプロセッサは処理を終了する。

【０１０２】

復号部５２７は、メモリリードライト装置５１を介してマイクロプロセッサ５０から暗号化命令を受け取り、キーコード入力部５２５が記憶しているキーコードを読み出す。更に、復号部５２７は、読み出したキーコードを復号鍵として用い、受け取った暗号化命令に復号アルゴリズムD_2を施して、復号化命令を生成する。復号部５２７は、生成した復号化命令を表示部５２１へ出力する。

【０１０３】

不揮発性メモリ５０５が記憶しているキーコードと、キーコード入力部５２５が受け付けるキーコードが同じであれば、ホストＰＣ５２は、マイクロプロセッサ５０から取得した暗号化命令を正しく復号することができる。

暗号部５２８は、外部記憶装置からオブジェクトファイル５３２を読み出す。また、キーコード入力部５２５が記憶しているキーコードを読み出す。暗号部５２８は、読み出したキーコードを暗号鍵として用い、読み出したオブジェクトファイルに暗号アルゴリズムE_2を施して、暗号化ファイルを生成する。暗号部２２９は、生成した暗号化ファイルをメモリリードライト装置５１を介してマイクロプロセッサ５０へ送出する。

【０１０４】

コンパイル部５２４は、ホストＰＣ５２上で動作するコンパイラ、アセンブラ及びリンカを機能的に示すもので、コンパイル部５２４は、メモリ操作コマンド入力部５２６から指示を受け取り、受け取った指示に対応するファイルを、外部記憶装置に記憶されているソースファイル５２３からを読み込む。コンパイル部５２４は、読み込んだソースファイルに、コンパイル、アセンブル及びリンク処理を施してオブジェクトファイル５３２生成し、生成したオブジェクトファイル５３２を外部記憶装置に書く。

【０１０５】

（動作）

ここでは、図３及び図１３に示すフローチャートを用いて、デバッグシステム５の動作について説明する。図３のステップＳ１０１からステップＳ１０８まで、デバッグシステム５の動作は、前述したデバッグシステム１の動作と同様であるため説明を省略し、図１３から説明する。

【０１０６】

コマンドが「メモリ書込み」であれば（ステップＳ１０８で「メモリ書込み」）、ホストＰＣ５２のメモリ操作コマンド入力部５２６は、書き込むデータファイルの指定を受け付ける（ステップＳ５０１）。メモリ操作コマンド入力部５２６は、指定されたオブジェクトファイルを、外部記憶装置から読み込み（ステップＳ５０２）、暗号部５２８に渡す。暗号部５２８は、オブジェクトファイルを受け取り、受け取ったオブジェクトファイルに、キーコード入力部５２５が記憶しているキーコードを暗号鍵として用い、暗号アルゴリズムE_2を施し暗号化する（ステップＳ５０３）。暗号部５２８は、メモリリードライト装置５１を介してマイクロプロセッサ５０に暗号化データを出力し（ステップＳ５０４）、マイクロプロセッサ５０の命令メモリ５０１及びデータメモリ５０３に書き込む（ステップＳ５０５）。

【０１０７】

コマンドが「メモリ読出し」であれば（ステップＳ１０８で「メモリ読出し」）、ホストＰＣ５２のメモリリードライト装置制御部５２２は、コマンドに対応する信号を、メモリリードライト装置５１を介してデバッグインターフェース５０７へ送出する。デバッグインターフェース５０７は、命令メモリ５０１及びデータメモリ５０３を読み出し、暗号化命令及び暗号化データを、メモリリードライト装置５１を介して復号部５２７へ出力する（ステップＳ５１１）。復号部５２７は、暗号化命令及び暗号化データを受け取り、キーコード入力部４２５が受け付けたキーコードを用いて、受け取った暗号化命令及び暗号化データを復号する（ステップＳ５１２）。復号部５２７は、復号した命令及びデータを表示部５２１へ出力し、表示部５２１は、命令及びデータを受け取りディスプレイに表示する（ステップＳ５１３）。その後、図３のステップＳ１０７に戻り処理を続け

る。

【０１０８】

コマンドが「終了」であれば、マイクロプロセッサは処理を終了する。

３．第３の実施の形態

本発明に係る第３の実施の形態として、デバッグシステム６について図面を参照して説明する。

＜構成＞

ここでは、デバッグシステム６の構成について説明する。デバッグシステム６は、マイクロプロセッサ６０、デバッグユニット６１、ホストＰＣ６２及び外部メモリ６３から構成される。マイクロプロセッサ６０と外部メモリ６３とは、ユーザが開発するＩＣカードの基板上に搭載されており、外部バスを介して互いに接続されている。デバッグユニット６１は、ケーブルを介してマイクロプロセッサ６０及びホストＰＣ６２と接続されている。外部メモリ６３は、ｎ－１個のメモリブロックに分割されており、各メモリブロックには、命令及びデータから成るコンピュータプログラムが記憶されている。各コンピュータプログラムは、マイクロプロセッサ６０により実行される。

デバッグシステム６では、複数の開発者が、それぞれの開発段階において固有のキーコードを用いてマイクロプロセッサ６０のデバッグを行うことが可能である。以下では、マイクロプロセッサ６０及びホストＰＣ６２について詳しく説明する。

【０１０９】

（マイクロプロセッサ６０）

図１４は、マイクロプロセッサ６０の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ６０は、命令メモリ６０１、命令実行ユニット６０２、データメモリ６０３、データ処理ユニット６０４、不揮発性メモリ６０５、復号化回路６０６、デバッグインターフェース６０７、バスコントローラ６０８及びアドレスデコーダ６０９から構成される。

【０１１０】

命令メモリ６０１は、具体的にはＲＡＭ及びＲＯＭであって、暗号化命令を記

憶している。命令メモリ６０１が記憶している暗号化命令は、予め、命令に暗号アルゴリズムE_3を施して生成したものである。暗号アルゴリズムE_3の一例はＤＥＳである。命令メモリ６０１は、バスを介して復号化回路６０６と接続されており、命令実行ユニット６０２の要求に従い、暗号化命令を復号化回路６０６へ出力する。更に、命令メモリ６０１は、バスを介してデバッグインターフェース６０７と接続されており、デバッグユニット６１を介して接続されたホストＰＣ６２上で動作するデバッガの要求を受けて、記憶している暗号化命令をデバッグインターフェース６０７及びデバッグユニット６１を介してホストＰＣ６２へ出力する。また、命令メモリ６０１は、デバッグインターフェース６０７から出力される暗号化命令を受け取り記憶する。

【０１１１】

命令実行ユニット６０２は、バスを介して復号化回路６０６と接続されており、復号化回路６０６から命令を受け取り、受け取った命令を解釈し、実行する。更に、命令実行ユニット６０２は、バスコントローラ６０８及び外部バスを介して外部メモリ６３と接続されており、外部メモリ６３の各メモリブロックが記憶している命令を、バスコントローラ６０８を介して読み出し、解釈し、実行する。

【０１１２】

データメモリ６０３は、具体的にはＲＯＭ又はＲＡＭであってデータを記憶している。データメモリ６０３は、バスを介してデータ処理ユニット６０４に接続されており、データ処理ユニット６０４からの要求を受けて、データ処理ユニット６０４へデータを出力する。データメモリ６０３は、データ処理ユニット６０４が出力する演算結果を受け取り記憶する。更に、データメモリ６０３は、バスを介してデバッグインターフェース６０７と接続されており、デバッグユニット６１を介して接続されたホストＰＣ６２上で動作するデバッガの要求を受けて、記憶しているデータをデバッグインターフェース６０７及びデバッグユニット６１を介してホストＰＣ６２へ出力する。また、データメモリ６０３は、デバッグインターフェース６０７から出力されるデータを受け取り記憶する。

【０１１３】

データ処理ユニット６０４は、バスを介してデータメモリ６０３と接続されており、データメモリ６０３からデータを読み出し、読み出したデータに演算処理を施し、演算結果をデータメモリ６０３に書き込む。更に、データ処理ユニット６０４は、外部バス及びバスコントローラ６０８を介して外部メモリ６３と接続されており、外部メモリ６３の各メモリブロックが記憶しているデータを、バスコントローラ６０８を介して読み出し、読み出したデータに演算処理を施し、演算結果を各メモリブロックに書き込む。

【０１１４】

不揮発性メモリ６０５は、「キーコード１」から「キーコードｎ」までのｎ個のキーコードと、「判定フラグＦ１」から「判定フラグＦｎ」までのｎ個の判定フラグとを記憶する領域を備え、各キーコードと各判定フラグとが書き込まれると、それらを所定の領域に記憶する。

「キーコード１」は、命令メモリ６０１が記憶している暗号化命令を復号するときに用いられる復号鍵である。「判定フラグＦ１」は、「キーコード１」が不揮発性メモリ６０５に書き込み済みか否かを判定するために用いるフラグであって、「キーコード１」が不揮発性メモリ６０５に書き込まれると、「判定フラグＦ１」が不揮発性メモリ６０５に書き込まれる。「キーコード２」は、外部メモリ６３のメモリブロック１に記憶されている暗号化命令を復号するときに用いられる復号鍵である。「判定フラグＦ２」は、「キーコード２」が不揮発性メモリ６０５に書き込み済みか否かを判定するために用いるフラグである。同様に、「キーコードｎ」は、外部メモリ６３のメモリブロックｎ－１に記憶されている暗号化命令を復号するときに用いられる復号鍵である。「判定フラグＦＮ」は、「キーコードＮ」が不揮発性メモリ６０５に書き込み済みか否かを判定するために用いるフラグである。

【０１１５】

なお、「キーコード１」から「キーコードｎ」は、それぞれ、一度だけ書き込みが可能であり、読み出し及び書き換えが出来ない。また、「判定フラグＦ１」から「判定フラグＦｎ」は、それぞれ、一度だけ書き込みが可能であり、書き換えが出来ない。

復号化回路６０６は、命令メモリ６０１及び外部メモリ６３の各メモリブロックに記憶されている暗号化命令を命令実行ユニット６０２が実行するために、復号化する回路である。復号化回路６０６は、命令メモリ６０１及び外部メモリ６３の各メモリブロックから暗号化命令を受け取る。復号化回路６０６は、対応するキーコードを不揮発性メモリから取得し、取得したキーコードを復号鍵として用いて暗号化命令に復号アルゴリズムD_3を施し復号化命令を生成する。ここで、復号アルゴリズムD_3は、暗号アルゴリズムE_3により生成された暗号文を復号するアルゴリズムである。復号化回路６０６は、生成した復号化命令を命令実行ユニット６０２へ出力する。

【０１１６】

デバッグインターフェース６０７は、命令メモリ６０１とデバッグユニット６１、データメモリ６０３とデバッグユニット６１及び不揮発性メモリ６０５とデバッグユニット６１との接続に用いられるインターフェースであって、不揮発性メモリ６０５を保護する。デバッグインターフェース６０７は、第２の実施の形態におけるデバッグインターフェース２０７と同様の機能を有するため、詳細な説明は省略する。

【０１１７】

バスコントローラ６０８は、マイクロプロセッサ６０の外部に設けられた外部メモリ６３と命令実行ユニット６０２、及び外部メモリ６３とデータ処理ユニット６０４との間で、外部バスを介して情報の受け渡しをする。

アドレスデコーダ６０９は、バスを介して命令メモリ６０１及び外部メモリ６３に接続されており、命令実行ユニット６０２から出力されるアドレスに対応して、命令メモリ６０１、外部メモリ６３の各メモリブロックを選択すると共に、選択されたメモリブロックに対応するキーコードを不揮発性メモリ６０５から読み出し、復号化回路６０６に出力する。

【０１１８】

（ホストＰＣ６２）

ホストＰＣ６２は、マイクロプロセッサ６０に対応したデバッガが動作するパーソナルコンピュータであり、マイクロプロセッサ６０の命令メモリ６０１を観

察可能な開発者が有するＰＣである。ホストＰＣ６２は、図１５に示す様に、表示部６２１とデバッグ部６２２とを備え、デバッグ部６２２は、キーコード入力部６２５、コマンド入力部６２６、復号部６２７、命令・データ入力部６２８及び暗号部６２９を含む。各部の機能はホストＰＣ２２の表示部２２１及びデバッグ部６２２と同様であるため、詳細な説明を省略する。

【０１１９】

＜動作＞

ここでは、図１６に示すフローチャートを用いてデバッグシステム６の動作について説明する。

ホストＰＣ６２のデバッグ部６２２が起動し、キーコード入力部６２５が、ユーザの操作によりキーコード番号Ｍの入力を受け付ける（ステップＳ６００）。ここで、Ｍは、１≦Ｍ≦ｎを満たす整数である。

【０１２０】

続いて、キーコード入力部６２５は、キーコードＮの入力を受け付け（ステップＳ６０１）、受け付けたキーコードＮを記憶する（ステップＳ６０２）。キーコード入力部６２５は、受け付けたキーコードＮを、デバッグユニット６１を介してデバッグインターフェース６０７へ送出する。デバッグインターフェース６０７は、キーコードＮを受け取ると、不揮発性メモリ６０５の「判定フラグＦＮ」の状態を読み、不揮発性メモリ６０５内のキーコードＮが書き込まれるべき領域に、キーコードＮが書き込み済みか否かを判断する（ステップＳ６０３）。前記領域にキーコードＮが書き込み済みでない場合（ステップＳ６０４でＮＯ）、デバッグインターフェース６０７は、受け取ったキーコードＮを不揮発性メモリ６０５に書き込む（ステップＳ６０５）。さらに、デバッグインターフェース６０７は、キーコードＮが書き込み済みであることを示す「判定フラグＦＮ」を不揮発性メモリ６０５に書き込む（ステップＳ６０６）。

【０１２１】

次に、コマンド入力部６２６が、ユーザからコマンドの入力を受け付ける（ステップＳ６０７）。ここで、コマンドの種類は、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であり、これらの内の何れか

一つがユーザにより選択される。コマンド入力部６２６は、選択されたコマンドを判断する（ステップＳ６０８）。以下、図７に示したフローチャートに続く。

【０１２２】

４、第４の実施の形態

本発明に係る第４の実施の形態として、デバッグシステム７について、図面を参照して説明する。

＜構成＞

ここでは、デバッグシステム７の構成について説明する。デバッグシステム７は、マイクロプロセッサ７０、デバッグユニット７１及びホストＰＣ７２から構成される。マイクロプロセッサ７０は、ユーザが開発するＩＣカードの基板上に搭載されており、デバッグユニット７１は、ケーブルを介してマイクロプロセッサ７０及びホストＰＣ７２と接続されている。以下では、マイクロプロセッサ７０及びホストＰＣ７２について詳細に説明する。

【０１２３】

（マイクロプロセッサ７０）

図１７は、マイクロプロセッサ７０の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ７０は、命令メモリ７０１、命令実行ユニット７０２、データメモリ７０３、データ処理ユニット７０４、不揮発性メモリ７０５、暗号化回路７０６、デバッグインターフェース７０７、セキュリティヒューズ７０８及びバッファ７０９から構成される。

【０１２４】

命令メモリ７０１は、具体的にはＲＡＭ及びＲＯＭであって命令を記憶している。命令メモリ７０１は、バスを介して命令実行ユニット７０２と接続されている。更に、命令メモリ７０１は、バスを介して暗号化回路７０６と接続されており、デバッグユニット７１を介して接続されたホストＰＣ７２上で動作するデバッガの要求を受けて、記憶している命令を暗号化回路７０６へ出力する。また、命令メモリ７０１は、暗号化回路７０６から出力される命令を受け取り記憶する。

【０１２５】

命令実行ユニット７０２は、バスを介して命令メモリ７０１と接続されており、命令メモリ７０１が記憶している命令を読み出し、解釈し、実行する。

データメモリ７０３は、具体的にはＲＯＭ又はＲＡＭであってデータを記憶している。データメモリ７０３は、バスを介してデータ処理ユニット７０４に接続されており、データ処理ユニット７０４からの要求を受けて、データ処理ユニット７０４へデータを出力する。データメモリ７０３は、データ処理ユニット７０４が出力する演算結果を受け取り記憶する。更に、データメモリ７０３は、バスを介して暗号化回路７０６と接続されており、デバッグユニット７１を介して接続されたホストＰＣ７２上で動作するデバッガの要求を受けて、記憶しているデータを暗号化回路７０６へ出力する。また、データメモリ７０３は、暗号化回路７０６から出力されるデータを受け取り記憶する。

【０１２６】

データ処理ユニット７０４は、バスを介してデータメモリ７０３と接続されており、データメモリ７０３からデータを読み出し、読み出したデータに演算処理を施し、演算結果をデータメモリ７０３に書き込む。

不揮発性メモリ７０５は、キーコードを記憶する領域と判定フラグを記憶する領域とを備え、キーコードと判定フラグとが書き込まれると、それらを所定の領域に記憶する。キーコードは、暗号化回路７０６による命令の暗号化及びデータの暗号化に用いられる暗号鍵であって、一度だけ書き込みが可能であり、読み出し及び書き換えが出来ない。判定フラグは、キーコードが不揮発性メモリ７０５に書き込み済みか否かを判定するために用いるフラグであって、キーコードが不揮発性メモリ７０５に書き込まれると、判定フラグが不揮発性メモリ７０５に書き込まれる。また、判定フラグは一度だけ書き込みが可能であり、書き換えが出来ない。

【０１２７】

暗号化回路７０６は、ホストＰＣ７２からの要求を受けて、命令メモリ７０１に記憶されている命令をデバッグインターフェース７０７が読み出すとき、また、データメモリ７０３に記憶されているデータをデバッグインターフェース７０７が読み出すときに命令及びデータを暗号化するための回路である。暗号化回路

７０６は、不揮発性メモリ７０５が記憶しているキーコードを暗号鍵として用いて命令メモリ７０１に記憶されている命令及びデータメモリ７０３に記憶されているデータに、暗号アルゴリズムE_4を施し暗号化命令及び暗号化データを生成する。ここで暗号アルゴリズムE_4は、例としてＤＥＳである。暗号化回路７０６は、生成した暗号化命令及び暗号化データをデバッグインターフェース７０７へ出力する。

【０１２８】

デバッグインターフェース７０７は、暗号化回路７０６とバッファ７０９、及び不揮発性メモリ７０５とバッファ７０９との接続に用いられ、暗号化回路７０６及び不揮発性メモリ７０５を保護する。デバッグインターフェース７０７は、第１の実施の形態におけるデバッグインターフェース１０７とほぼ同様の機能を有するが、デバッグインターフェース１０７と異なり、暗号化回路７０６から暗号化命令及び暗号化データを受け取ると、受け取った暗号化命令及び暗号化データをバッファ７０９に出力する。

【０１２９】

セキュリティヒューズ７０８は、「０」又は「１」のフラグであって、「０」は、セキュリティヒューズが切断された状態であり、バッファ７０９の出力を抑制することを示す。「１」は、バッファ７０９は通常通り出力することを示す。セキュリティヒューズ７０８は、初期状態ではフラグは、「１」に設定されている。セキュリティヒューズ７０８は、デバッグユニット７１を介してホストＰＣ７２の比較部７２８から指示を受けてフラグを「１」から「０」へ書き換える。なお、「１」から「０」に書き換えられたフラグを再度「１」に書き換えることは出来ない。

【０１３０】

バッファ７０９は、バスを介してデバッグインターフェース７０７及びセキュリティヒューズ７０８と接続されている。バッファ７０９は、セキュリティヒューズ７０８の状態を読み出す。読み出したセキュリティヒューズ７０８の状態が「０」の場合、バッファ７０９は、デバッグインターフェース７０７から暗号化命令と暗号化データとを受け取ると、デバッグユニット７１との接続を切断する

。セキュリティヒューズ７０８の状態が「１」の場合、バッファ７０９は通常通りにデバッグユニット７１と接続され、デバッグインターフェース７０７から受け取る暗号化命令と暗号化データとをデバッグユニット７１へ出力する。

【０１３１】

（ホストＰＣ７２）

ホストＰＣ７２は、マイクロプロセッサ７０に対応したデバッガが動作するパーソナルコンピュータである。

図１８は、ホストＰＣ７２の構成を示すブロック図である。同図に示す様に、ホストＰＣ７２は、表示部７２１、デバッグ部７２２及びカウンタ７４１を備える。デバッグ部７２２は、ホストＰＣ７２上で動作するデバッガを機能的に示すもので、キーコード入力部７２３、コマンド入力部７２４、復号部７２５、命令・データ入力部７２６、指定回数記憶部７２７及び比較部７２８を含む。

【０１３２】

表示部７２１は、ディスプレイユニットを含み、各種の画面をディスプレイに表示する。表示部７２１は、デバッグシステム１の表示部１２１と同様の機能を有するため、詳細な説明を省略する。

カウンタ７４１は、外部記憶装置に記憶されており、キーコード入力部７２３が、前回受け付けたキーコードと異なるキーコードを何回受け付けたのかをカウントする。カウンタ７４１は、キーコード入力部７２３からの指示を受け、記憶している数値に１を加算する。

【０１３３】

キーコード入力部７２３は、キーボード及びマウス等を含む。キーコード入力部７２３は、内部に記憶領域を備え、キーコード入力部７２３が前回入力を受け付けたキーコード（以下「前回キーコード」と呼称する）を前記記憶領域に記憶している。キーコード入力部７２３は、表示部７２１にキーコードの入力を受け付けるための画面が表示されている状態において、ユーザの操作により、キーボード及びマウスを介したキーコードの入力を受け付ける。キーコード入力部７２３は、キーコードの入力を受け付けると、受け付けた当該キーコードと前回キーコードとが一致するか否かを判定する。不一致の場合、キーコード入力部７２３

は、カウンタ７４１に対して、記憶している数値に１を加算する信号を出力し、前記領域に記憶されている前回キーコードに当該キーコードを上書きする。

【０１３４】

また、キーコード入力部７２３は、当該キーコードを、デバッグユニット７１、バッファ７０９及びデバッグインターフェース７０７を介して不揮発性メモリ７０５に送出する。

コマンド入力部７２４は、第１の実施の形態におけるコマンド入力部１２４と同様の機能を有するため、ここでは説明を省略する。

【０１３５】

復号部７２５は、デバッグユニット７１及びバッファ７０９を介して、デバッグインターフェース７０７から暗号化命令を受け取る。また、復号部７２５は、キーコード入力部７２３が記憶しているキーコードを読み出す。更に、復号部７２５は、読み出したキーコードを復号鍵として用い、受け取った暗号化命令に復号アルゴリズムD_4を施して、復号化命令を生成する。ここで、復号アルゴリズムD_4は、暗号アルゴリズムE_4により生成された暗号文を復号するアルゴリズムである。復号部７２５は、生成した復号化命令を表示部７２１へ出力する。同様にして、復号部７２５は、暗号化データを取得し、取得した暗号化データにキーコードを復号鍵として用い、取得した暗号化データに復号アルゴリズムD_4を施して、復号化データを生成する。復号部７２５は、生成した復号化データを表示部７２１へ出力する。

【０１３６】

命令・データ入力部７２６は、第１の実施の形態における命令・データ入力部１２６と同様の機能を有するため、ここでは説明を省略する。

指定回数記憶部７２７は、指定回数を示す数値を保持する。ここで、指定回数とはキーコード入力部７２３がユーザから受け付けるキーコードが前回キーコードと異なる場合において、異なるキーコードを受け付けた回数が当該指定回数を越えた場合にデバッグを停止するために用いる数値である。

【０１３７】

比較部７２８は、カウンタ７４１が記憶している数値と指定回数記憶部７２７

が記憶している数値とを読み、比較する。カウンタ７４１が記憶している数値が、指定回数記憶部７２７が記憶している数値よりも大きい場合、比較部７２８は、デバッグユニット７１を介してフラグを「０」に書き換える信号をセキュリティヒューズ７０８へ出力する。

【０１３８】

＜動作＞

ここでは、図１９及び図２０に示すフローチャートを用いて、デバッグシステム７の動作について説明する。

ホストＰＣ７２のキーコード入力部７２３は、判定フラグの状態を読み（ステップＳ７０１）、不揮発性メモリ７０５にキーコードが書き込み済みか否か判断する。不揮発性メモリ７０５にキーコードが書き込み済みの場合（ステップＳ７０２でＹＥＳ）、キーコード入力部７２３は、ユーザからキーコードの入力を受け付ける（ステップＳ７０３）。キーコード入力部７２３は、受け付けたキーコードを記憶する（ステップＳ７０４）。

【０１３９】

キーコード入力部７２３は、内部に記憶している前回キーコードを読み（ステップＳ７０５）、受け付けたキーコードが前回キーコードに一致するか否か判断する。一致しない場合（ステップＳ７０６でＮＯ）、カウンタ７４１は、キーコード入力部７２３からの信号を受けて、記憶している数値に１を加算する（ステップＳ７０７）。次に、比較部７２８は、カウンタ７４１が記憶している数値と指定回数記憶部７２７が記憶している指定回数とを読み出し、比較する（ステップＳ７０８）。カウンタ７４１が記憶している値が、指定回数よりも大きい場合（ステップＳ７０９でＹＥＳ）、比較部７２８は、セキュリティヒューズ７０８のフラグを「０」に書き換える指示を出力し、セキュリティヒューズを切断する（ステップＳ７１０）。カウンタ７４１が記憶している値が、指定回数よりも小さい場合（ステップＳ７０９でＮＯ）、ステップＳ７０３に戻り処理を続ける。

【０１４０】

キーコード入力部７２３は、判定フラグを読み出した結果、不揮発性メモリ７０５にキーコードが書き込まれていない場合（ステップＳ７０２でＮＯ）、ユー

ザからキーコードの入力を受け付ける（ステップＳ７２１）。キーコード入力部７２３は、受け付けたキーコードを記憶すると共に（ステップＳ７２２）、デバッグユニット７１、バッファ７０９及びデバッグインターフェース７０７を介して不揮発性メモリ７０５に受け付けたキーコードを書き込む（ステップＳ７２３）。次に、キーコード入力部７２３は、デバッグユニット７１、バッファ７０９及びデバッグインターフェース７０７を介して不揮発性メモリに、キーコードが書き込み済みであることを示す判定フラグを書き込む（ステップＳ７２４）。

【０１４１】

次に、ホストＰＣ７２のコマンド入力部７２４が、ユーザからコマンドの入力を受け付ける（ステップＳ７２５）。ここで、コマンドの種類は、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であり、これらの内の何れか一つがユーザにより選択される。コマンド入力部７２４は、選択されたコマンドを判断する（ステップＳ７２６）。以下、図４に示したフローチャートに続く。

【０１４２】

受け付けたキーコードが前回キーコードに一致する場合は（ステップＳ７０６でＹＥＳ）、ステップＳ７２５に続く。

５．第５の実施の形態

本発明に係る第５の実施の形態として、デバッグシステム８について、図面を参照して説明する。デバッグシステム８は、デバッグシステム７におけるキーコード比較処理を、ホストＰＣ側が行うのではなく、マイクロプロセッサ側が行うことが特徴である。

【０１４３】

＜構成＞

ここでは、デバッグシステム８の構成について説明する。デバッグシステム８は、マイクロプロセッサ８０、デバッグユニット８１及びホストＰＣ８２から構成される。マイクロプロセッサ８０は、ユーザが開発するＩＣカードの基板上に搭載されており、デバッグユニット８１は、ケーブルを介してマイクロプロセッサ８０及びホストＰＣ８２と接続されている。

【０１４４】

ホストＰＣ８２は、表示部８２１及びデバッグ部８２２から構成され、デバッグ部８２２は、更に、キーコード入力部８２３、コマンド入力部８２４、復号部８２５及び命令・データ入力部８２６から構成される。なお、ホストＰＣ８２の構成は図示していない。ホストＰＣ８２の各構成要素は、第１の実施の形態におけるホストＰＣ１２の各構成要素と同様の機能を有するため説明を省略する。

【０１４５】

以下では、マイクロプロセッサ８０の構成について説明する。

（マイクロプロセッサ８０）

図２１は、マイクロプロセッサ８０の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ８０は、命令メモリ８０１、命令実行ユニット８０２、データメモリ８０３、データ処理ユニット８０４、不揮発性メモリ８０５、暗号化回路８０６、デバッグインターフェース８０７、前回キーコード記憶部８０８、指定回数記憶部８０９、カウンタ８１０、比較部８１１、セキュリティヒューズ８１２及びバッファ８１３から構成される。

【０１４６】

命令メモリ８０１、命令実行ユニット８０２、データメモリ８０３、データ処理ユニット８０４、不揮発性メモリ８０５、暗号化回路８０６及びバッファ８１３は、それぞれ、第４の実施の形態における命令メモリ７０１、命令実行ユニット７０２、データメモリ７０３、データ処理ユニット７０４、不揮発性メモリ７０５、暗号化回路７０６及びバッファ７０９と同様の機能を有するため、ここでは説明を省略する。

【０１４７】

デバッグインターフェース８０７は、暗号化回路８０６とバッファ８１３、不揮発性メモリ８０５とバッファ８１３、及び前回キーコード記憶部８０８とカウンタ８１０の接続に用いられる。

前回キーコード記憶部８０８は、キーコードを記憶する領域を備え、前回、バッファ８１３から受け取ったキーコード（以下、前回キーコードと呼称する）を記憶する。前回キーコード記憶部８０８は、ホストＰＣ８２のキーコード入力部

８２３が受け付けたキーコードを、デバッグユニット８１及びバッファ８１３を介してデバッグインターフェース８０７から受け取り、受け取った当該キーコードと記憶している前回キーコードとを比較する。前回キーコード記憶部８０８は、両者が異なる場合に、カウンタ８１０に対して記憶している数値に１を加算する信号を出力し、更に、比較部８１１に対してカウンタ８１０が記憶している数値と指定回数記憶部８０９が記憶している数値とを比較する信号を出力する。

【０１４８】

指定回数記憶部８０９は、予め、一度だけ書き込みが可能な指定回数を示す数値を記憶している。指定回数とは、ホストＰＣ８２がユーザから受け付けるキーコードが前回受け付けたキーコードと異なる場合において、異なるキーコードを受け付けた回数が当該指定回数を越えた場合にセキュリティヒューズ８１２を切断し、デバッグを停止するために用いる数値である。

【０１４９】

カウンタ８１０は、ホストＰＣ８２が、前回キーコード記憶部８０８が記憶しているキーコードと異なるキーコードを受け付けた回数をカウントする。カウンタ８１０は、前回キーコード記憶部８０８からの指示を受け、記憶している数値に１を加算する。

比較部８１１は、前回キーコード記憶部８０８からの指示を受け、カウンタ８１０が記憶している数値と指定回数記憶部８０９が記憶している数値とを読み出し、比較する。カウンタ８１０が記憶している数値が、指定回数記憶部８０９が記憶している数値よりも大きい場合、比較部８１１は、セキュリティヒューズ８１２に対して、フラグを「０」に書き換える信号を出力する。

【０１５０】

セキュリティヒューズ８１２は、セキュリティヒューズ７０８と同様に「０」又は「１」に設定されたフラグであって、「０」は、セキュリティヒューズが切断された状態であり、バッファ８１３の出力を抑制することを示す。「１」は、バッファ８１３は通常通りに出力することを示す。セキュリティヒューズ８１３は、初期状態ではフラグは、「１」に設定されている。セキュリティヒューズ８１３は、比較部８１１から指示を受けてフラグを「１」から「０」へ書き換える

。なお、「１」から「０」に書き換えられたフラグを再度「１」に書き換えることは出来ない。

【０１５１】

＜動作＞

ここでは、図２２及び図２０に示すフローチャートを用いて、デバッグシステム８の動作について説明する。

ホストＰＣ８２のキーコード入力部８２３は、不揮発性メモリ８０５の判定フラグの状態を読み出し（ステップＳ８０１）、不揮発性メモリ８０５にキーコードが書き込み済みか否か判断する。キーコードが書き込み済みの場合（ステップＳ８０２でＹＥＳ）、キーコード入力部８２３は、ユーザからキーコードの入力を受け付ける（ステップＳ８０３）。キーコード入力部８２３は、受け付けたキーコードを記憶する（ステップＳ８０４）。

【０１５２】

続いて、キーコード入力部８２３は、受け付けたキーコードを、デバッグユニット８０、バッファ８１３及びデバッグインターフェース８０７を介して、前回キーコード記憶部８０８へ送出する。前回キーコード記憶部８０８は、内部に記憶している前回キーコードを読む（ステップＳ８０５）。前回キーコード記憶部８０８は、受け付けたキーコードが前回キーコードに一致するか否か判断する。一致しない場合（ステップＳ８０６でＮＯ）、前回キーコード記憶部８０８は、カウンタ８１０へ信号を出力する。カウンタ８１０は、前回キーコード記憶部８０８からの信号を受けて、記憶している数値に１を加算する（ステップＳ８０７）。次に、比較部８１１は、カウンタ８１０が記憶している数値と指定回数記憶部８０９が記憶している指定回数とを読み出し、比較する。カウンタ８１０が記憶している値が、指定回数よりも大きい場合（ステップＳ８０８でＹＥＳ）、比較部８１１は、セキュリティヒューズ８１２のフラグを「１」から「０」に書き換える指示を出力し、セキュリティヒューズを切断する（ステップＳ８０９）。カウンタ８１０が記憶している値が、指定回数よりも小さい場合（ステップＳ８０８でＮＯ）、ステップＳ８０３に戻り処理を続ける。

【０１５３】

不揮発性メモリ８０５から読み出した判定フラグを判断し、キーコードが書き込み済みでない場合（ステップＳ８０２でＮＯ）、図２０のステップＳ７２１に続く。

前回キーコード記憶部８０８が、受け付けたキーコードが、内部に記憶している前回キーコードに一致する場合（ステップＳ８０６でＹＥＳ）、図２０のステップＳ７２５に続く。

【０１５４】

６．第６の実施の形態

本発明に係る第６の実施の形態として、デバッグシステム９について、図面を参照して説明する。

＜構成＞

ここでは、デバッグシステム９の構成について説明する。デバッグシステム９は、マイクロプロセッサ９０、デバッグユニット９１及びホストＰＣ９２から構成される。マイクロプロセッサ９０は、ユーザが開発するＩＣカードの基板上に搭載されて接続されており、デバッグユニット９１は、ケーブルを介してマイクロプロセッサ９０及びホストＰＣ９２と接続されている。

【０１５５】

ホストＰＣ９２は、表示部及びデバッグ部から構成され、デバッグ部は、更に、キーコード入力部、コマンド入力部、復号部及び命令・データ入力部から構成される。なお、ホストＰＣ９２の構成は図示していない。ホストＰＣ９２の各構成要素は、第１の実施の形態におけるホストＰＣ１２の各構成要素と同様の機能を有するため説明を省略する。

【０１５６】

以下では、マイクロプロセッサ９０の構成について説明する。

図２３は、マイクロプロセッサ９０の構成を示すブロック図である。マイクロプロセッサ９０は、命令メモリ９０１、命令実行ユニット９０２、データメモリ９０３、データ処理ユニット９０４、不揮発性メモリ９０５、暗号化回路９０６、デバッグインターフェース９０７及びセレクタ９０８から構成される。命令メモリ９０１、命令実行ユニット９０２、データメモリ９０３、データ処理ユニッ

ト９０４、不揮発性メモリ９０５、暗号化回路９０６及びデバッグインターフェース９０７は、それぞれ、第１の実施の形態におけるマイクロプロセッサ１０の命令メモリ１０１、命令実行ユニット１０２、データメモリ１０３、データ処理ユニット１０４、不揮発性メモリ１０５、暗号化回路１０６及びデバッグインターフェース１０７と同様の機能を有するため、ここでは説明を省略する。

【０１５７】

セレクタ９０８は、バスを介して不揮発性メモリ９０５と接続されている。更に、セレクタ９０８は、バスＡ１を介して命令メモリ９０１と接続され、バスＡ２を介してデータメモリ９０３と接続されている。また、セレクタ９０８は、暗号化バスＢ１及び暗号化バスＢ２を介して暗号化回路９０６と接続されている。暗号化バスＢ１は、命令の読み出し及び書き込みに用いるバスであり、暗号化回路９０６と命令メモリ９０１とを接続する。暗号化バスＢ２は、データの読み出し及び書き込みに用いるバスであり、暗号化回路９０６とデータメモリ９０３とを接続する。

【０１５８】

セレクタ９０８は、不揮発性メモリ９０５の判定フラグを読み出して判定フラグの状態に応じて、以下に示す様にバスを選択する。

不揮発性メモリ９０５に判定フラグが書き込まれていない場合、すなわち、不揮発性メモリ９０５にキーコードが書き込まれていない場合、セレクタ９０８は、命令読み出し処理及び命令書き込み処理においては、バスＡ１を選択する。命令読み出し処理では、セレクタ９０８は、バスＡ１を介して命令メモリ９０１から命令を読み出し、読み出した命令をデバッグインターフェース９０７へ出力する。命令書き込み処理では、セレクタ９０８は、デバッグインターフェース９０７から命令を受け取り、受け取った命令をバスＡ１を介して命令メモリ９０１へ書き込む。データ読み出し処理及びデータ書き込む処理においては、バスＡ２を選択する。データ読み出し処理では、セレクタ９０８は、バスＡ２を介してデータメモリ９０３からデータを読み出し、読み出したデータをデバッグインターフェース９０７へ出力する。データ書き込み処理では、セレクタ９０８は、デバッグインターフェース９０７からデータを受け取り、受け取ったデータをバスＡ１

を介して命令メモリ９０１へ書き込む。

【０１５９】

不揮発性メモリ９０５に判定フラグが書き込まれている場合、すなわち、不揮発性メモリ９０５にキーコードが書き込み済みの場合、セレクタ９０８は命令読み出し処理おいては、暗号化バスＢ１を選択する。セレクタ９０８は、暗号化バスＢ１を介して命令メモリ９０１から命令を読み出し、読み出した命令を暗号化回路９０６へ出力する。セレクタ９０８は、暗号化バスＢ１を介して暗号化回路９０６から暗号化命令を受け取り、受け取った暗号化命令をデバッグインターフェース９０７へ出力する。セレクタ９０８は、命令書き込み処理においては、バスＡ１を選択する。セレクタ９０８は、デバッグインターフェース９０７から命令を受け取り、受け取った命令をバスＡ１を介して命令メモリ９０１へ書き込む。セレクタ９０８は、データ読み出し処理においては、暗号化バスＢ２を選択する。セレクタ９０８は、暗号化バスＢ２を介してデータメモリ９０３からデータを読み出し、読み出したデータを暗号化回路９０６へ出力する。セレクタ９０８は、暗号化バスＢ２を介して暗号化回路９０６から暗号化データを受け取り、受け取った暗号化データをデバッグインターフェース９０７へ出力する。セレクタ９０８は、データ書き込み処理においては、バスＡ２を選択する。セレクタ９０８は、デバッグインターフェース９０７からデータを受け取り、受け取ったデータをバスＡ２を介してデータメモリ９０３へ書き込む。

【０１６０】

これにより、不揮発性メモリ９０５にキーコードが書き込み済みの場合は、暗号化回路９０６により暗号化された暗号化命令及び暗号化データが、デバッグインターフェース９０７及びデバッグユニット９１を介してホストＰＣ９２へ送出され、不揮発性メモリ９０５にキーコードが書き込み済みでない場合は、暗号化されていない命令及びデータが、デバッグインターフェース９０７及びデバッグユニット９１を介してホストＰＣ９２へ送出される。

【０１６１】

＜動作＞

ここでは、図２４、図２５及び図４に示すフローチャートを用いてデバッグシ

ステム９の動作について説明する。

ホストＰＣ９２のデバッグ部が起動し、デバッグ部からの信号を受けて、マイクロプロセッサ９０のデバッグインターフェース９０７は、不揮発性メモリ９０５の判定フラグの状態を読み出し（ステップＳ９０１）、不揮発性メモリ９０５にキーコードが書き込み済みか否かを判断する。

【０１６２】

キーコードが書き込み済みの場合（ステップＳ９０２でＹＥＳ）、ホストＰＣ９２のキーコード入力部は、ユーザからキーコードの入力を受け付け（ステップＳ９０９）、受け付けたキーコードを、デバッグユニット９１を介してデバッグインターフェース９０７へ送出し、ステップＳ９０７へ続く。キーコードが書き込み済みでない場合（ステップＳ９０２でＮＯ）、デバッグインターフェース９０７は、キーコードが書き込み済みでないことを示す信号を、デバッグユニット９１を介してホストＰＣ９２のデバッグ部へ送出する。

【０１６３】

デバッグ部は、キーコードを不揮発性メモリ９０５に書き込むか否かをユーザに問うための画面を表示部へ出力し、当該画面が表示されている状態に於いて、デバッグ部のキーコード入力部は、ユーザからの選択を受け付ける。キーコードを書き込まない選択を受け付けた場合（ステップＳ９０３でＮＯ）、図２５のフローチャートに続く。

【０１６４】

ホストＰＣ９２のコマンド入力部が、ユーザからコマンドの入力を受け付ける（ステップＳ９１０）。ここで、コマンドの種類は、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であり、これらの内の何れか一つがユーザにより選択される。コマンド入力部は、選択されたコマンドを判断する（ステップＳ９１１）。

【０１６５】

コマンドが「命令表示」であれば（ステップＳ９１１で「命令表示」）、デバッグ部は、デバッグユニット９１を介して、デバッグインターフェース９０７へコマンドに対応する信号を送出する。デバッグインターフェース９０７は、命令

メモリから命令を読み出し（ステップＳ９１２）、セレクタ９０８は、バスＡ１を選択して命令をデバッグインターフェース９０７及びデバッグユニット９１を介してホストＰＣ９２へ出力する（ステップＳ９１３）。ホストＰＣ９２の表示部は、命令を受け取り、受け取った命令を画面に表示する（ステップＳ９１４）。その後、ステップＳ９１０に戻り処理を続ける。

【０１６６】

コマンドが「命令書込み」であれば（ステップＳ９１１で「命令書込み」）、ホストＰＣ９２の命令・データ入力部は、ユーザから命令の入力を受け付ける（ステップＳ９２１）。命令・データ入力部は、受け付けた命令を、デバッグユニット９１を介してデバッグインターフェース９０７へ出力する（ステップＳ９２２）。セレクタ９０８は、バスＡ１を選択し、デバッグインターフェース９０７は、バスＡ１を介して命令を命令メモリ９０１に書き込む（ステップＳ９２３）。その後、ステップＳ９１０に戻り処理を続ける。

【０１６７】

コマンドが「データ表示」であれば（ステップＳ９１１で「データ表示」）、デバッグ部は、デバッグユニット９１を介してデバッグインターフェース９０７へコマンドに対応する信号を出力する。デバッグインターフェース９０７は、データメモリ９０３からデータを読み出し（ステップＳ９３１）、セレクタ９０８は、バスＡ２を選択してデータをデバッグインターフェース９０７及びデバッグユニット９１を介してホストＰＣ９２へを出力する（ステップＳ９３２）。ホストＰＣ９２の表示部は、データを受け取り、受け取ったデータを画面に表示する（ステップＳ９３３）。その後、ステップＳ９１０に戻り処理を続ける。

【０１６８】

コマンドが「データ書込み」であれば（ステップＳ９１１で「データ書込み」）、ホストＰＣ９２の命令・データ入力部は、ユーザからデータの入力を受け付ける（ステップＳ９４１）。命令・データ入力部は、受け付けたデータを、デバッグユニット９１を介してデバッグインターフェース９０７へ出力する。（ステップＳ９４２）。セレクタ９０８は、バスＡ２を選択して、デバッグインターフェース９０７は、バスＡ２を介してデータをデータメモリ９０３に書き込む（ス

テップＳ９４３）。その後、ステップＳ９１０に戻り処理を続ける。

【０１６９】

コマンドが「終了」であれば（ステップＳ９１１で「終了」）、処理を終了する。

ここで、図２４のステップＳ９０３に戻る。キーコードを書き込む場合（ステップＳ９０３でＹＥＳ）、キーコード入力部は、ユーザからキーコードの入力を受け付け（ステップＳ９０４）、受け付けたキーコードを、内部に記憶すると共に、デバッグユニット９１を介してデバッグインターフェース９０７へ送出する。デバッグインターフェース９０７は、キーコードを受け取り、受け取ったキーコードを不揮発性メモリ９０５に書き込む（ステップＳ９０５）。更に、デバッグインターフェース９０７は、キーコードが書き込み済みであることを示す判定フラグを不揮発性メモリ９０５に書き込む（ステップＳ９０６）。

【０１７０】

次に、ホストＰＣ９２のコマンド入力部が、ユーザからコマンドの入力を受け付ける（ステップＳ９０７）。ここで、コマンドの種類は、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であり、これらの内の何れか一つがユーザにより選択される。コマンド入力部は、選択されたコマンドを判断する（ステップＳ９０８）。

【０１７１】

以下は、図４に示した第１の実施の形態におけるデバッグシステム１の動作と同様の処理であるため、ここでは図４のフローチャートを用いてデバッグシステム１との相違点を中心に説明する。

コマンドが「命令表示」であれば（ステップＳ９０８で「命令表示」）、デバッグインターフェース９０７は、命令メモリ９０１から命令を読み出し（ステップＳ１０９）、セレクタ９０８は、暗号化バスＢ１を選択して命令を暗号化回路９０６へ出力する。暗号化回路９０６は、命令に暗号化処理を施し暗号化命令を生成する（ステップＳ１１０）。暗号化回路９０６は、生成した暗号化命令を、暗号化バスＢ１を介してデバッグインターフェース９０７へ出力し、デバッグインターフェース９０７は、デバッグユニット９１を介して暗号化命令をホストＰ

Ｃ９２へ出力する（ステップＳ１１１）。以下は、デバッグシステム１と同様である。

【０１７２】

コマンドが「命令書込み」であれば（ステップＳ９０８で「命令書込み」）、ホストＰＣ９２の命令・データ入力部は、ユーザから命令の入力を受け付ける（ステップＳ１２１）。命令・データ入力部は、受け付けた命令を、デバッグユニット９１を介してデバッグインターフェース９０７へ出力する（ステップＳ１２２）。セレクタ９０８は、バスＡ１を選択して、デバッグインターフェース９０７は、バスＡ１を介して命令を命令メモリ９０１に書き込む（ステップＳ１２３）。その後、ステップＳ９０７に戻り処理を続ける。

【０１７３】

コマンドが「データ表示」であれば（ステップＳ９０８で「データ表示」）、デバッグインターフェース９０７は、データメモリ９０３からデータを読み出し（ステップＳ１３１）、セレクタ９０８は、暗号化バスＢ２を選択して読み出したデータを暗号化回路９０６へ出力する。暗号化回路９０６は、データに暗号化処理を施して暗号化データを生成する（ステップＳ１３２）。暗号化回路９０６は、生成した暗号化データを、暗号化バスＢ２を介してデバッグインターフェース９０７へ出力し、デバッグインターフェース９０７は、デバッグユニット９１を介して暗号化データをホストＰＣ９２へ出力する（ステップＳ１３３）。以下は、デバッグシステム１と同様である。

【０１７４】

コマンドが「データ書込み」であれば（ステップＳ９０８で「データ書込み」）、ホストＰＣ９２の命令・データ入力部は、ユーザからデータの入力を受け付ける（ステップＳ１４１）。命令・データ入力部は、受け付けたデータを、デバッグユニット９１を介してデバッグインターフェース９０７へ出力する（ステップＳ１４２）。セレクタ９０８は、バスＡ２を選択し、デバッグインターフェース９０７はバスＡ２を介してデータをデータメモリ９０３に書き込む（ステップＳ１４３）。その後、ステップＳ９０７に戻り処理を続ける。

【０１７５】

コマンドが「終了」であれば（ステップＳ９０８で「終了」）、処理を終了する。

７．第７の実施の形態

本発明に係る第７の実施の形態として、デバッグシステム１５について図面を参照して説明する。

【０１７６】

デバッグシステム１５は、マイクロプロセッサ１００、デバッグユニット１１０及びホストＰＣ１２０から構成される。マイクロプロセッサ１００は、ユーザが開発するＩＣカードの基板上に搭載されて接続されており、デバッグユニット１１０は、ケーブルを介してマイクロプロセッサ１００及びホストＰＣ１２０と接続されている。

【０１７７】

（マイクロプロセッサ１００の構成）

図２５は、マイクロプロセッサ１００の構成を示すブロック図である。同図に示す様に、マイクロプロセッサ１００は、命令メモリ１００１、命令実行ユニット１００２、データメモリ１００３、データ処理ユニット１００４、不揮発性メモリ１００５、復号化回路１００６、デバッグインターフェース１００７及びキャッシュ１００８から構成される。

【０１７８】

マイクロプロセッサ１００は、復号化回路１００６と命令実行ユニット１００２との間にキャッシュ１００８を有することが特徴である。命令メモリ１００１、命令実行ユニット１００２、データメモリ１００３、データ処理ユニット１００４、不揮発性メモリ１００５、復号化回路１００６及びデバッグインターフェース１００７は、それぞれ、第２の実施の形態におけるマイクロプロセッサ２０の各構成要素と同様の機能を有する。以下ではマイクロプロセッサ２０との相違点を中心に説明する。

【０１７９】

キャッシュ１００８は、復号化回路１００６と命令実行ユニット１００２との間に設けられたキャッシュメモリであって、命令実行ユニット１００３における

命令の実行時間が、復号化回路１００６における暗号化命令の復号処理よりも長い場合に、命令実行ユニット１００２における命令の実行中に復号化回路１００６から受け取る命令を内部に蓄積する。

【０１８０】

命令実行ユニット１００２は、キャッシュ１００８が蓄積している命令を読み出して、読み出した命令を実行する。

デバッグシステム１５の動作については、デバッグシステム２と同様であるため、説明を省略する。

８．まとめ

以上説明したように、本発明のデバッグシステム及びマイクロプロセッサによれば、デバッガが起動するホストＰＣ上でユーザから入力されたキーコードを用いて、マイクロプロセッサとホストＰＣとの間で命令及びデータを暗号化して伝送することができる。本発明のデバッグシステム及びマイクロプロセッサによれば、悪意のあるユーザがマイクロプロセッサをデバッグユニットに接続してマイクロプロセッサを解析しようとしても、マイクロプロセッサから取得できるのは、暗号化命令及び暗号化データであり、暗号化命令及び暗号化データを取得した場合であっても、マイクロプロセッサの不揮発性メモリに記憶されている正しいキーコードを知らなければ復号することができず、マイクロプロセッサの内部情報を解析することができない。更に、マイクロプロセッサ設計者、デバッグシステム設計者、プログラム開発者なども正しいキーコードを知ることはなく、キーコード設定者のみがマイクロプロセッサの内部情報を解析することができる。これにより、課金処理を行うような、高度なセキュリティが要求されるシステムにおいてもデバッグとセキュリティの維持を両立することができる。

【０１８１】

以上、本発明を上記実施の形態に基づき説明してきたが、本発明は上記実施の形態に限定されず、以下のような場合も本発明に含まれる。

（１）上記実施の形態において、デバッグの対象であるマイクロプロセッサは、ＩＣカードの基板上に搭載されているが、ＩＣカードの基板に限定されないのは勿論であり、ユーザが開発するターゲット基板であればよい。

【０１８２】

（２）上記実施の形態では、デバッガのコマンドは、「命令表示」、「命令書込み」、「データ表示」、「データ書込み」及び「終了」であるが、本発明において、デバッガのコマンドは、これらに限定されない。

（３）第２の実施の形態における命令書き込み処理は、デバッグ部２２２の命令・データ入力部２２８が受け付けた命令を暗号化してマイクロプロセッサ２０の命令メモリ２０１に格納しているが、デバッガ部２２２は、外部記憶装置に記憶されているソースファイルを指定し、コンパイル部２２４が指定されたソースファイルを読み込み、オブジェクトファイルを生成し、生成したオブジェクトファイルを、暗号化して、暗号化オブジェクトファイルをマイクロプロセッサ２０の命令メモリ２０１に格納する構成としてもよい。また、予めコンパイル部２２４が、暗号化した暗号化オブジェクトを外部記憶装置へ格納しておき、デバッグ部２２２は、外部記憶装置に格納されている暗号化オブジェクトファイルを読み出してマイクロプロセッサ２０の命令メモリ２０１に書き込むように構成してもよい。

【０１８３】

（４）また、第２の実施の形態において、不揮発性メモリ２０５が保持するキーコードは、読み出しが不可能であり、且つ、書き換えが可能であっても良い。この場合、コンパイラで指定したキーコードが分からない限り、不揮発性メモリ２０５が保持するキーコードを書き換えても。命令が正常に実行できなくなり、セキュリティ上の問題は無い。

【０１８４】

（５）また、第２の実施の形態＜変形例３＞において、メモリリードライト装置５１の対象は、マイクロプロセッサ５０に限定されない。例えば、マイクロプロセッサ５０の外部に接続されたメモリもメモリリードライト装置５１の対象になる。

（６）また、第３の実施の形態では、デバッグを行う複数の者に対して、予め固有のキーコードとキーコード番号とが秘匿に通知されているとしてもよい。任意のキーコードを入力するのではなく、予め他人には秘匿に設定されて保持され

たキーコードを用いる構成も本発明に含まれる。

【０１８５】

また、キーコードの数とメモリブロックの数とは１対１に対応していなくてもよい。秘匿したいレベルに応じた数のキーコードによりメモリが管理される構成であれば、１個のキーコードが複数のメモリブロックに対応する構成も本発明に含まれる。

（７）命令及びデータの暗号化に用いる暗号アルゴリズムはＤＥＳに限定されない。公開鍵暗号方式であってもよい。

【０１８６】

（８）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリ等に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は、前記デジタル信号を電気通信回路、無線又は有線通信回路、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

【０１８７】

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、前記コンピュータプログラムを記憶しており、前記マイクロプロセッサが前記コンピュータプログラムに従って動作するとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は、前記プログラム又は前記デジタル信号をネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【０１８８】

（９）第１の実施の形態から第７の実施の形態を適宜組み合わせた構成も本発明に含まれる。また、各実施の形態に上記変形例を組み合わせた構成も本発明に含まれる。

【０１８９】

【発明の効果】

以上説明したように、本発明は、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと、前記マイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするために用いられるホストコンピュータとから構成されるデバッグシステムである。

【０１９０】

前記マイクロプロセッサは、前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の領域を備える一度だけ書き込みが可能な不揮発性メモリを備え、前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、受け取った鍵情報を前記不揮発性メモリに書き込み、前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する。

【０１９１】

前記ホストコンピュータは、利用者から鍵情報の入力を受け付け、前記鍵情報を内部に記憶すると共に、前記マイクロプロセッサへ送出し、記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送する。

この構成によると、前記不揮発性メモリに書き込まれた鍵情報は、読み出し及び書き換えが不可能である。前記デバッグシステムにおいて、前記マイクロプロセッサ及び前記ホストコンピュータは、読み出し及び書き換えが不可能な鍵情報を用いて前記プログラム情報をセキュアに伝送するため、前記ホストコンピュータから初めて鍵情報を入力した利用者のみが、前記マイクロプロセッサのプログラム情報を取得することが出来る。それにより、前記マイクロプロセッサを用いるシステムの開発段階において、複数の開発者が関わる場合であっても、前記利用者のみが前記マイクロプロセッサのプログラム情報を取得して、セキュリティ

を保ちつつデバッグすることができる。

【０１９２】

また、本発明は、デバッグするために用いられるホストコンピュータと接続され、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサである。前記マイクロプロセッサは、プログラム、データ又はプログラム及びデータを示す前記プログラム情報を記憶しており、前記プログラム情報を読み出し、読み出したプログラム情報に従って動作する。前記マイクロプロセッサは、前記プログラム情報をセキュアに扱うために用いられる鍵情報を記憶する為の領域を備える一度だけ書き込みが可能な不揮発性メモリを備え、前記不揮発性メモリが鍵情報を記憶していない場合に、前記ホストコンピュータから鍵情報を受け取り、受け取った鍵情報を前記不揮発性メモリに書き込み、前記不揮発性メモリが記憶している鍵情報を用いて、前記ホストコンピュータとの間で前記プログラム情報をセキュアに伝送する。

【０１９３】

この構成によると、前記マイクロプロセッサの前記不揮発性メモリが記憶する鍵情報は、一度書き込まれると読み出し及び書き換えが不可能であるため、前記マイクロプロセッサは、接続されたホストコンピュータとの間で、前記プログラム情報をセキュアに伝送することができる。

ここで、前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、前記マイクロプロセッサは、前記フラグ情報を読み出し、読み出した前記フラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記ホストコンピュータから鍵情報を受け付け、受け付けた鍵情報を前記不揮発性メモリに書き込むように構成してもよい。

【０１９４】

この構成によると、前記伝送手段は、前記不揮発性メモリのフラグを読み出すことにより、前記不揮発性メモリに鍵情報が書き込まれているか否かを判断することができる。

ここで、前記マイクロプロセッサは、前記不揮発性メモリに記憶されている鍵情報を用いて、前記プログラム情報を暗号化し、暗号化されたプログラム情報を

出力するように構成してもよい。

【０１９５】

この構成によると、プログラム情報を暗号化するために用いる鍵情報は、前記不揮発性メモリが記憶している鍵情報である。前記不揮発性メモリが記憶している鍵情報は、前述の通り、一度だけ書き込みが可能で読み出し及び書き換えが出来ない。そのため前記マイクロプロセッサは、セキュリティの高い状態でプログラム情報を前記ホストコンピュータへ伝送することが可能である。

【０１９６】

ここで、前記マイクロプロセッサは、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成したプログラム、データ又はプログラム及びデータに従って動作し、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を前記ホストコンピュータへ伝送するように構成してもよい。

【０１９７】

この構成によると、前記マイクロプロセッサは、既に暗号化されたプログラム情報を記憶しているため、前記ホストコンピュータとの間でセキュリティを保った状態でプログラム情報を伝送することができる。更に、暗号化されたプログラム情報を実行する場合は、暗号化されたプログラム情報を、前記不揮発性メモリが記憶している鍵情報を用いて復号することで、プログラム情報記憶手段がプログラム情報を暗号化した状態で記憶していてもプログラムを実行することができる。

【０１９８】

ここで、前記マイクロプロセッサは、更に、動作の結果生成された生成データを、鍵情報を用いて暗号化し、暗号化された生成データを内部に書き込むように構成してもよい。

この構成によると、前記不揮発性メモリが暗号化されたデータを記憶している場合であっても、暗号化されたデータを、鍵情報を用いて復号し、演算後のデー

タを再度鍵情報を用いて暗号化することでプログラム情報のセキュリティを保ちつつプログラム情報を実行することができる。

【０１９９】

ここで、前記マイクロプロセッサは、前記プログラムのみが鍵情報を用いて暗号化された暗号化プログラムを含むプログラム情報を記憶しており、前記外部装置との通信経路を備えるように構成してもよい。

この構成によると、前記プログラム情報記憶部は外部装置と接続されているがプログラムは暗号化されているため、プログラムのセキュリティは保たれる。データは暗号化されていないため、必要に応じて外部装置からデータを取得することが可能である。

【０２００】

ここで、前記鍵情報は１以上の部分鍵情報から構成され、前記プログラムは、複数の部分プログラムから構成され、各部分プログラムは、前記１以上の部分鍵情報の何れかに対応しており、前記マイクロプロセッサは、複数の部分プログラムが、対応する部分鍵情報を用いて暗号化された暗号化部分プログラムを含むプログラム情報を記憶しており、前記不揮発性メモリから部分鍵情報を読み出し、読み出した部分鍵情報に対応する１以上の暗号化部分プログラムを読み出し、読み出した１以上の暗号化部分プログラムを、前記部分鍵情報を用いて復号して部分プログラムを生成し、生成した部分プログラムに従って動作するように構成してもよい。

【０２０１】

この構成によると、部分プログラム毎に異なる鍵情報が設定されており、複数の開発者がそれぞれ互いに知ることのない鍵情報を設定することで部分プログラム毎にセキュリティを保った状態で前記ホストコンピュータへ伝送が可能である。

ここで、前記マイクロプロセッサは、さらに、前記ホストコンピュータからの要求に応じて、暗号化されたプログラム情報の出力を抑制するように構成してもよい。

【０２０２】

この構成によると、プログラム情報が暗号化された状態であっても、前記ホストコンピュータからの要求により前記ホストコンピュータへのプログラム情報の出力を抑制することができるため、悪意のある解析者が前記ホストコンピュータからプログラム情報を取得するのを防止することができる。

ここで、前記マイクロプロセッサは、さらに、鍵情報に係る情報であり、暗号化されたプログラム情報の出力の抑制を示す抑制条件を記憶しており、前記ホストコンピュータから受け付けた前記鍵情報が、前記抑制条件を満たす場合に、暗号化されたプログラム情報の出力を抑制するように構成してもよい。

【０２０３】

この構成によると、プログラム情報が暗号化された状態であっても、前記鍵情報が前記抑制条件を満たす場合に、前記ホストコンピュータへのプログラム情報の出力を抑制することができるため、悪意のある解析者が前記ホストコンピュータからプログラム情報を取得するのを防止することができる。ここで、上述のマイクロプロセッサと比較すると、上述のマイクロプロセッサは、ホストコンピュータからの指示を受けてプログラム情報の出力を抑制するのに対し、当該マイクロプロセッサプロセッサは、出力を抑制するための判断を当該マイクロプロセッサ自身が行うため、よりセキュリティが高い。

【０２０４】

ここで、前記不揮発性メモリは、鍵情報が書き込み済みか否かを示すフラグ情報を記憶しており、前記マイクロプロセッサは、前記フラグ情報を読み出し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていないことを示す場合に、前記プログラム情報を読み出し、読み出したプログラム情報を出力し、読み出したフラグ情報が前記不揮発性メモリに鍵情報が書き込まれていることを示す場合に、前記プログラム情報を読み出し、読み出したプログラム情報を前記鍵情報で暗号化し、暗号化されたプログラム情報を出力するように構成してもよい。

【０２０５】

この構成によると、前記マイクロプロセッサは、前記プログラム情報を暗号化して出力するか、暗号化せずに出力するかを選択することができる。それにより

、前記不揮発性メモリに鍵情報が記憶されていない状態において、プログラム開発者はプログラム情報を暗号化せずにデバッグを行い、その後、他の利用者が鍵情報を設定することができる。これを、ＩＣカードを用いたサービスシステムの例を用いて説明する。ＩＣカードに搭載されるマイクロプロセッサの開発者、プログラム開発者及びＩＣカード開発者は、開発段階においてプログラム情報を暗号化せず取得し、デバッグを行うことができる。その後、ＩＣカードを用いたサービス業者がプログラム情報を書き込み、更に、前記不揮発性メモリに鍵情報を書き込む。これ以後は、当該サービス業者のみがプログラム情報を取得することができる。

【０２０６】

ここで、前記マイクロプロセッサは、更に、キャッシュメモリを備える、前記マイクロプロセッサは、前記プログラム、データ又はプログラム及びデータが鍵情報を用いて暗号化されて生成されたプログラム情報を記憶しており、前記不揮発性メモリから鍵情報を読み出し、読み出した鍵情報を用いて、プログラム情報を復号してプログラム、データ又はプログラム及びデータを生成し、生成した前記プログラム、データ又はプログラム及びデータを前記キャッシュメモリに書き込む。前記マイクロプロセッサは、実行ユニットにおける実行速度に応じて前記キャッシュメモリから前記プログラム、データ又はプログラム及びデーを読み出し、読み出したプログラム、データ又はプログラム及びデータに従って動作する。前記マイクロプロセッサは、プログラム、データ又はプログラム及びデータが暗号化されて生成されたプログラム情報を前記ホストコンピュータに伝送するように構成してもよい。

【０２０７】

この構成によると、前記実行手段における復号処理時間が長く、実行処理時間が短い場合であっても、復号したプログラムを前記キャッシュメモリに蓄積することにより実行処理をスムーズに継続することができる。

また、本発明は、外部に秘匿するプログラム情報を記憶しているマイクロプロセッサと接続され、前記マイクロプロセッサの動作をデバッグするホストコンピュータである。前記ホストコンピュータは、利用者から鍵情報の入力を受け付け

、前記鍵情報を、内部に記憶すると共に前記マイクロプロセッサへ送出し、記憶している前記鍵情報を用いて、前記マイクロプロセッサとの間で前記プログラム情報をセキュアに伝送することを特徴とする。

【０２０８】

この構成によると利用者から受け付けた鍵情報を前記マイクロプロセッサへ送出し、当該鍵情報を用いて前記プログラム情報を伝送するので、当該利用者以外の者に対してセキュリティが保たれる。

ここで、前記ホストコンピュータは、前記マイクロプロセッサから、前記鍵情報を用いて暗号化されたプログラム情報を受け取り、前記暗号化されたプログラム情報に、記憶している前記鍵情報を用いて復号し、復号したプログラム情報を表示するように構成してもよい。

【０２０９】

この構成によると、前記利用者以外の者が前記プログラム情報を復号することは不可能であり、セキュリティを保った状態で前記利用者は前記プログラム情報を取得し、デバッグを行うことができる。

ここで、前記ホストコンピュータは、更に、利用者から、プログラム、データ又はプログラム及びデータを示すプログラム情報の入力を受け付け、受け付けた前記プログラム情報に、記憶している前記鍵情報を用いて暗号化し、暗号化したプログラム情報を前記マイクロプロセッサへ出力するように構成してもよい。

【０２１０】

この構成によると、プログラム情報を暗号化して前記マイクロプロセッサに伝送するため、セキュリティを保った状態で前記プログラム情報を前記マイクロプロセッサへ伝送することができる。

ここで、前記ホストコンピュータは、更に、ソースプログラムを記憶しており、前記ソースプログラムを変換してプログラムを示すプログラム情報を生成し、生成した前記プログラム情報に、前記鍵情報を用いて暗号化し、暗号化したプログラム情報を前記マイクロプロセッサへ伝送するように構成してもよい。

【０２１１】

この構成によると、前記ホストコンピュータがソースプログラムをコンパイル

して、更に、生成したオブジェクトプログラムを暗号化して前記マイクロプロセッサへ伝送するため、セキュリティを保った状態で前記マイクロプロセッサへプログラムを書き込むことができる。

ここで、前記マイクロプロセッサは、更に、鍵情報に係る情報で、前記マイクロプロセッサとの間での、前記暗号化されたプログラム情報の伝送の停止を示す停止条件を記憶しており、受け付けた前記鍵情報が、前記停止条件を満たす場合に、前記マイクロプロセッサに対して、前記暗号化されたプログラム情報の出力を抑制することを示す要求を出力するように構成してもよい。

【０２１２】

この構成によると、前記ホストコンピュータは、前記停止条件として異なる鍵情報が入力された回数を示す数値を記憶しておき、何度も異なる鍵情報が入力された場合に、前記マイクロプロセッサとの間の暗号化されたプログラム情報の伝送を停止することができる。これにより、何度も異なる鍵情報を入力して暗号化されたプログラム情報を復号しようとする悪意のある者が、プログラム情報を復号して、改竄することを防止することができる。

【図面の簡単な説明】

【図１】

マイクロプロセッサ１０の構成を示すブロック図である。

【図２】

ホストＰＣ１２の構成を示すブロック図である。

【図３】

デバッグシステム１の動作を示すフローチャートであり、図４に続く。

【図４】

デバッグシステム１の動作を示すフローチャートであり、図３から続く。

【図５】

マイクロプロセッサ２０の構成を示すブロック図である。

【図６】

ホストＰＣ２２の構成を示すブロック図である。

【図７】

デバッグシステム２の動作を示すフローチャートであり、図３から続く。

【図８】

マイクロプロセッサ３０の構成を示すブロック図である。

【図９】

マイクロプロセッサ４０の構成を示すブロック図である。

【図１０】

ホストＰＣ４２の構成を示すブロック図である。

【図１１】

デバッグシステム４の動作を示すフローチャートであり、図３から続く。

【図１２】

ホストＰＣ５２の構成を示すブロック図である。

【図１３】

デバッグシステム５の動作を示すフローチャートであり、図３から続く。

【図１４】

マイクロプロセッサ６０の構成を示すブロック図である。

【図１５】

ホストＰＣ６２の構成を示すブロック図である。

【図１６】

デバッグシステム６の動作を示すフローチャートであり、図７に続く。

【図１７】

マイクロプロセッサ７０の構成を示すブロック図である。

【図１８】

ホストＰＣ７２の構成を示すブロック図である。

【図１９】

デバッグシステム７の動作を示すフローチャートであり、図４及び図２０に続く。

【図２０】

デバッグシステム７の動作を示すフローチャートであり、図１９及び図２２から続く。

【図２１】

マイクロプロセッサ８０の構成を示すブロック図である。

【図２２】

デバッグシステム８の動作を示すフローチャートであり、図４及び図２０に続く。

【図２３】

マイクロプロセッサ９０の構成を示すブロック図である。

【図２４】

デバッグシステム９の動作を示すフローチャートであり、図４及び図２５に続く。

【図２５】

デバッグシステム９の動作を示すフローチャートであり、図２４から続く。

【図２６】

マイクロプロセッサ１００の構成を示すブロック図である。

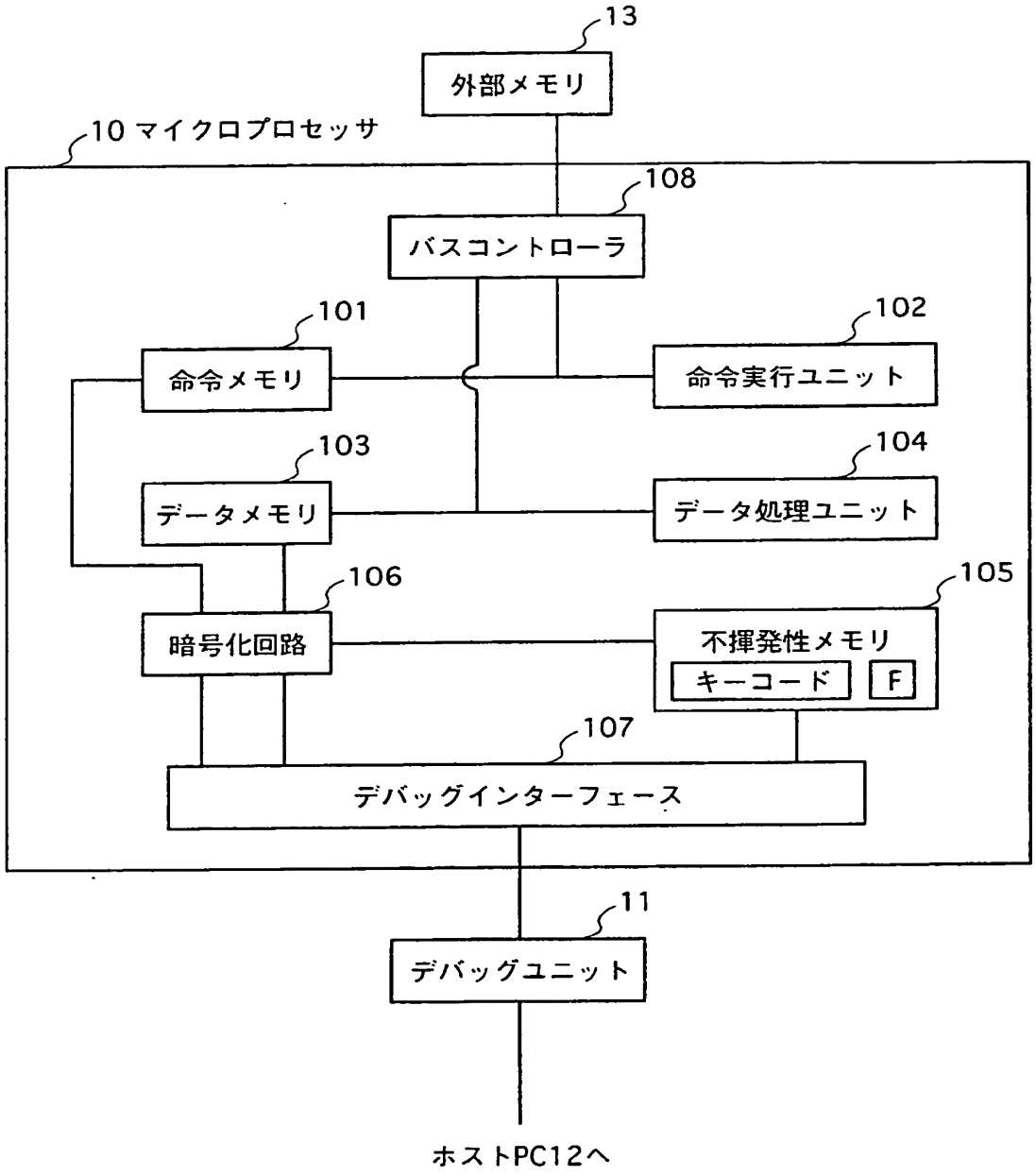
【符号の説明】

１０　マイクロプロセッサ
１１　デバッグユニット
１２　ホストＰＣ
１３　外部メモリ
２０　マイクロプロセッサ
２１　デバッグユニット
２２　ホストＰＣ
２３　外部メモリ
３０　マイクロプロセッサ
３１　デバッグユニット
３２　ホストＰＣ
３３　外部メモリ
４０　マイクロプロセッサ
４１　デバッグユニット

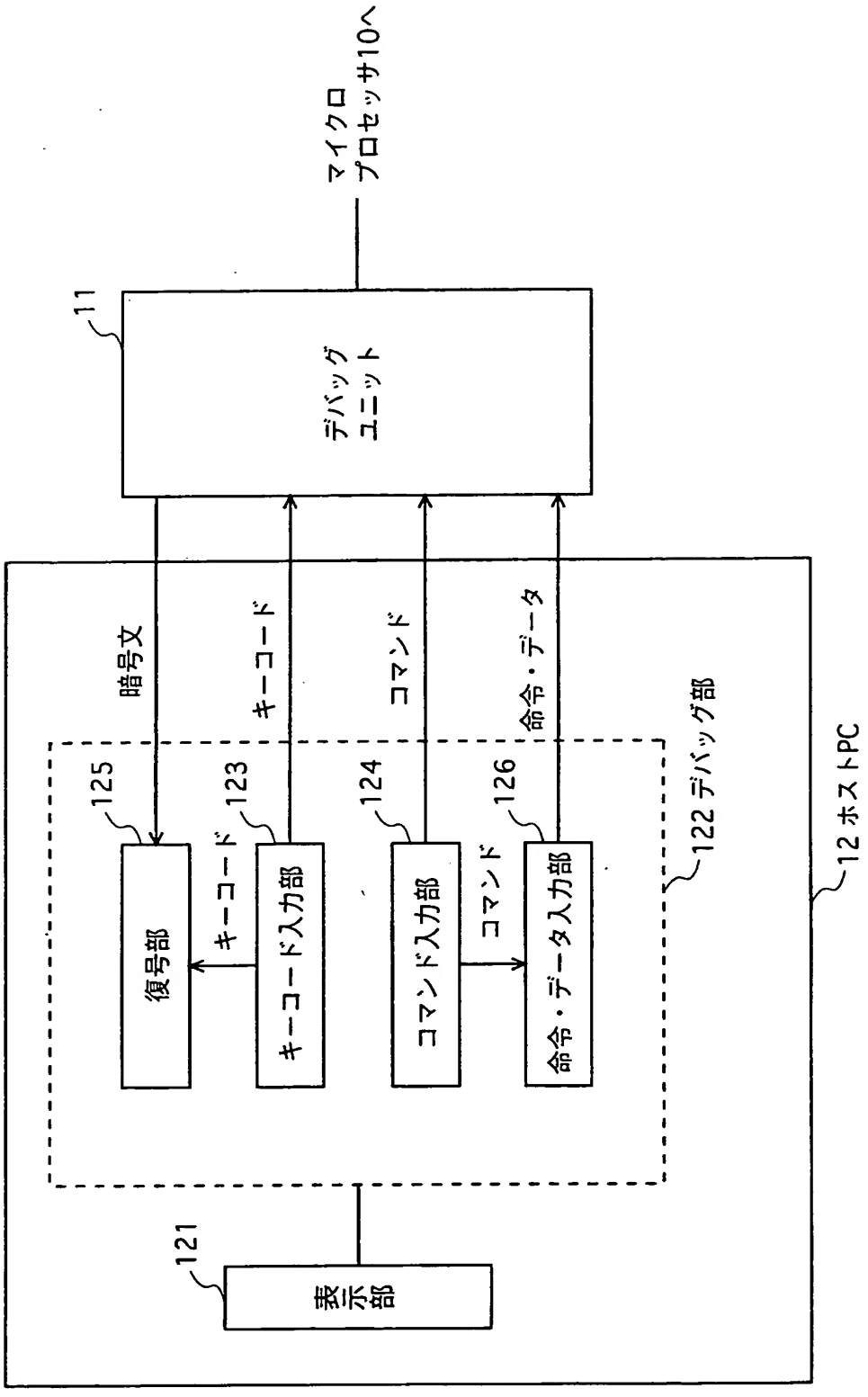
４２　ホストＰＣ
５０　マイクロプロセッサ
５１　メモリリードライト装置
５２　ホストＰＣ
６０　マイクロプロセッサ
６１　デバッグユニット
６２　ホストＰＣ
６３　外部メモリ
７０　マイクロプロセッサ
７１　デバッグユニット
７２　ホストＰＣ
８０　マイクロプロセッサ
８１　デバッグユニット
８２　ホストＰＣ
９０　マイクロプロセッサ
９１　デバッグユニット
９２　ホストＰＣ
１００　マイクロプロセッサ
１１０　デバッグユニット
１２０　ホストＰＣ

【書類名】　図面

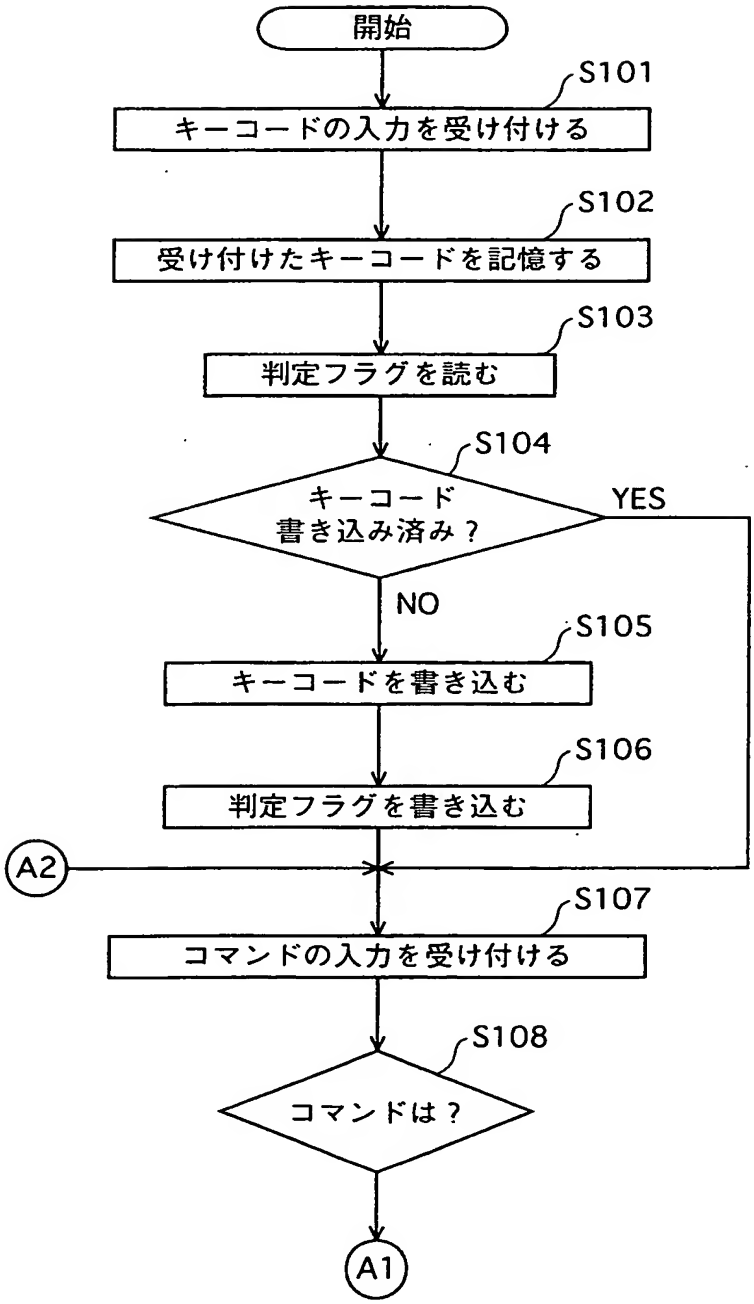
【図１】


13
外部メモリ
10 マイクロプロセッサ
108
バスコントローラ
101
命令メモリ
102
命令実行ユニット
103
データメモリ
104
データ処理ユニット
106
暗号化回路
105
不揮発性メモリ
キーコード
F
107
デバッグインターフェース
11
デバッグユニット
ホストPC12へ

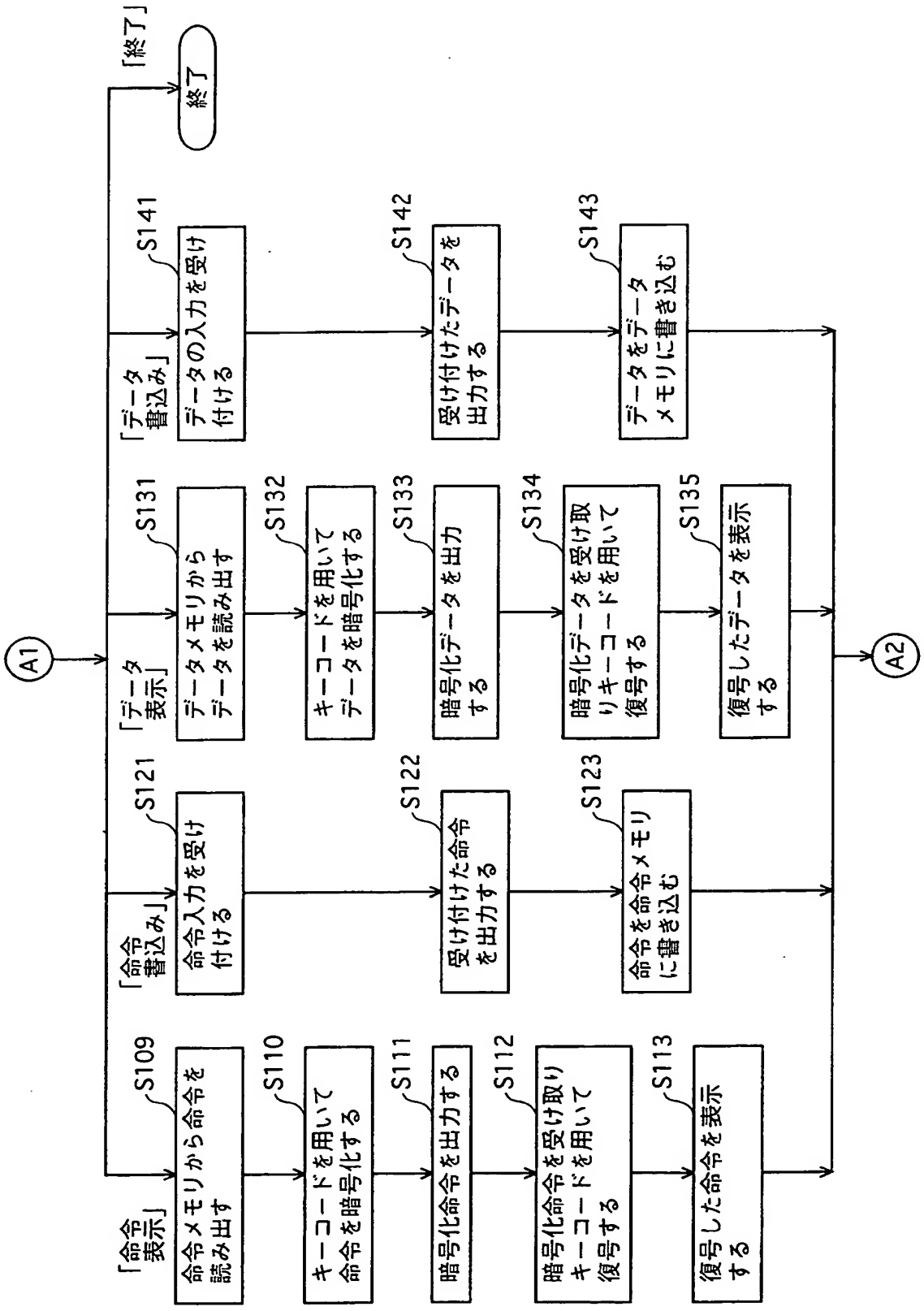
【図２】


マイクロプロセッサ10へ
11
デバッグユニット
暗号文
キーコード
コマンド
命令・データ
125
123
124
126
復号部
キーコード入力部
コマンド入力部
命令・データ入力部
122 デバッグ部
12 ホストPC
121
表示部

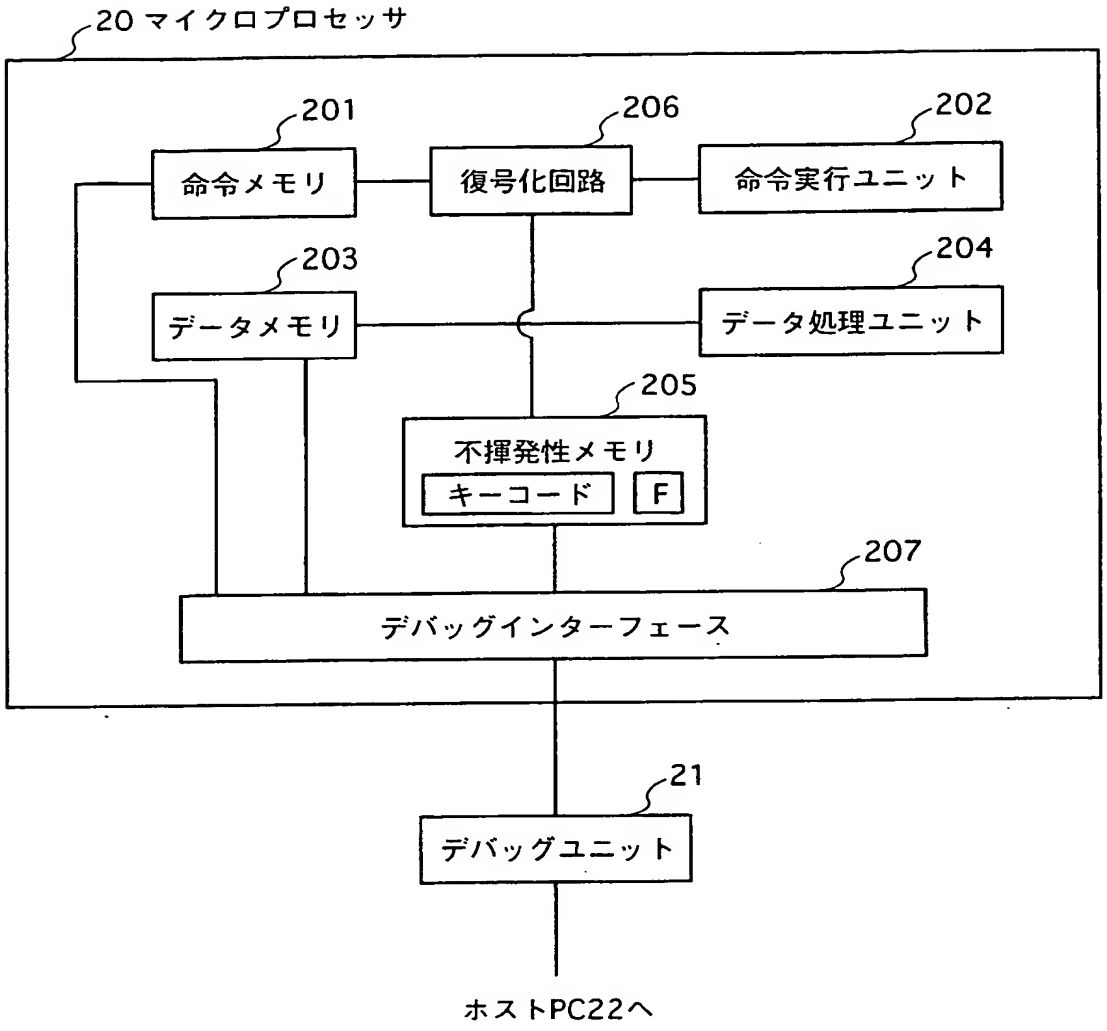
【図３】


開始
S101
キーコードの入力を受け付ける
S102
受け付けたキーコードを記憶する
S103
判定フラグを読む
S104
キーコード
書き込み済み？
YES
NO
S105
キーコードを書き込む
S106
判定フラグを書き込む
A2
S107
コマンドの入力を受け付ける
S108
コマンドは？
A1

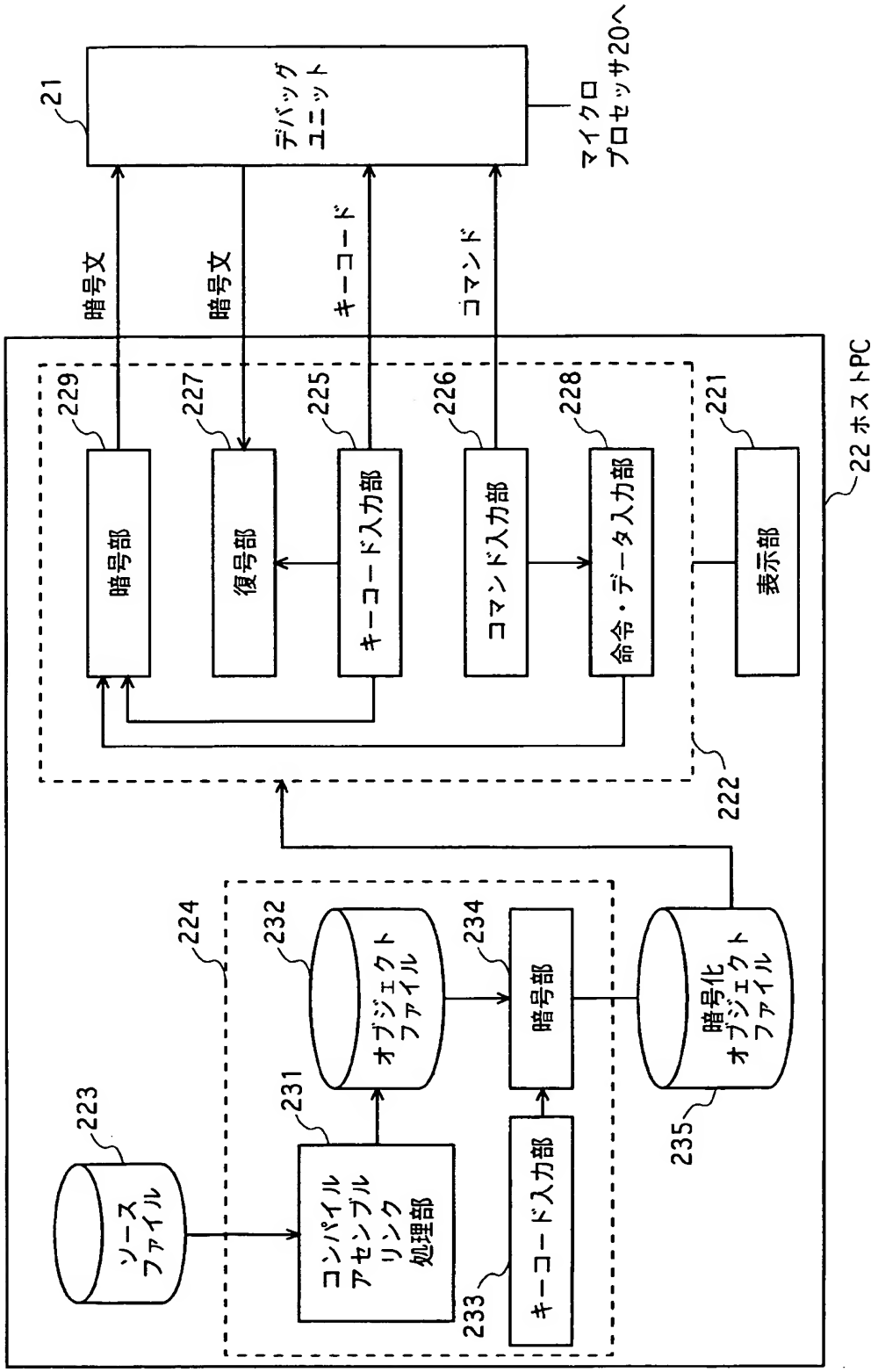
【図４】


「終了」
終了
「データ書込み」
S141
データの入力を受け付ける
S142
受け付けたデータを出力する
S143
データをデータメモリに書き込む
「データ表示」
S131
データメモリからデータを読み出す
S132
キーコードを用いてデータを暗号化する
S133
暗号化データを出力する
S134
暗号化データを受け取りキーコードを用いて復号する
S135
復号したデータを表示する
「命令書込み」
S121
命令入力を受け付ける
S122
受け付けた命令を出力する
S123
命令を命令メモリに書き込む
「命令表示」
S109
命令メモリから命令を読み出す
S110
キーコードを用いて命令を暗号化する
S111
暗号化命令を出力する
S112
暗号化命令を受け取りキーコードを用いて復号する
S113
復号した命令を表示する
A1
A2

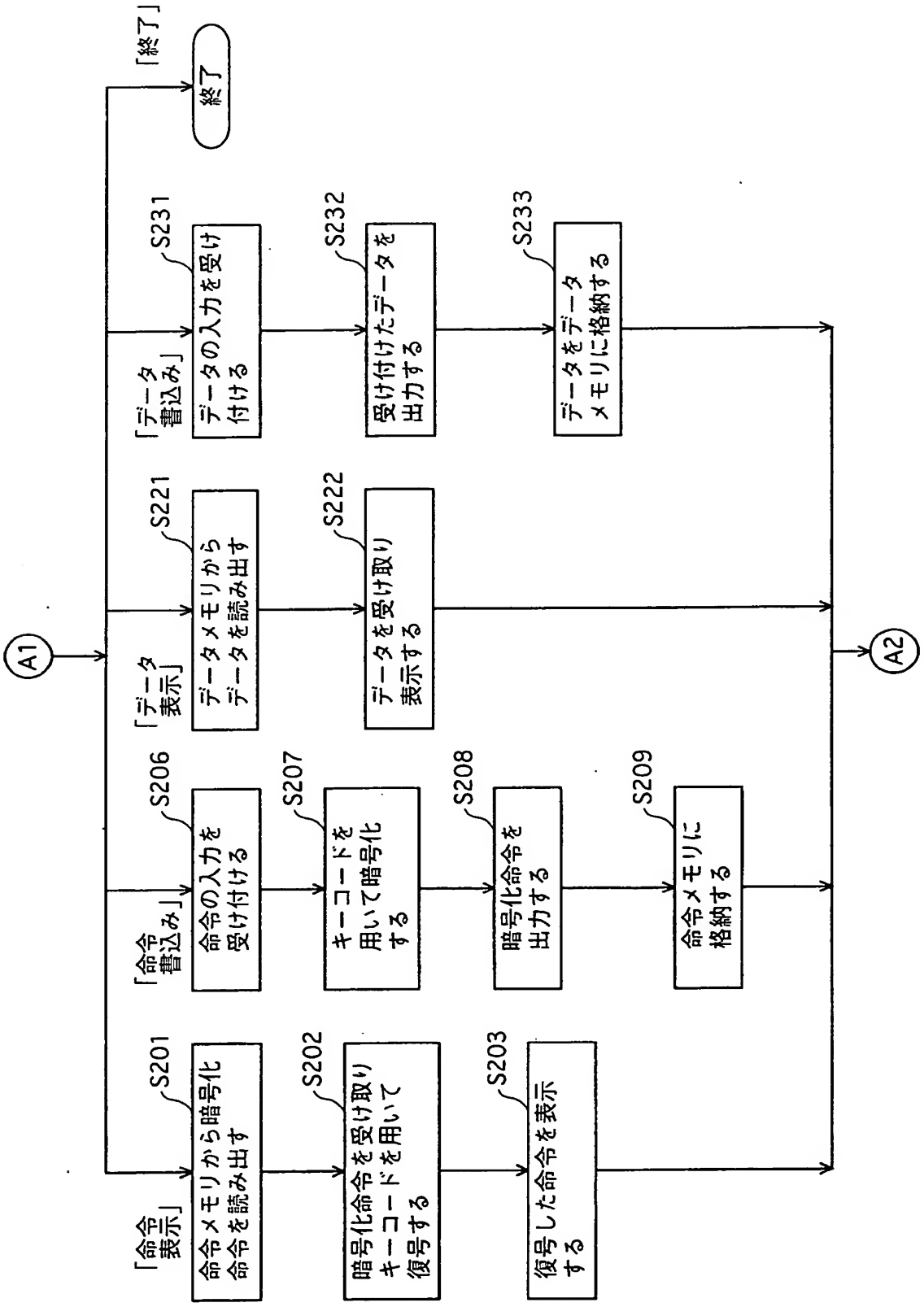
【図５】


20 マイクロプロセッサ
201
命令メモリ
206
復号化回路
202
命令実行ユニット
203
データメモリ
204
データ処理ユニット
205
不揮発性メモリ
キーコード
F
207
デバッグインターフェース
21
デバッグユニット
ホストPC22へ

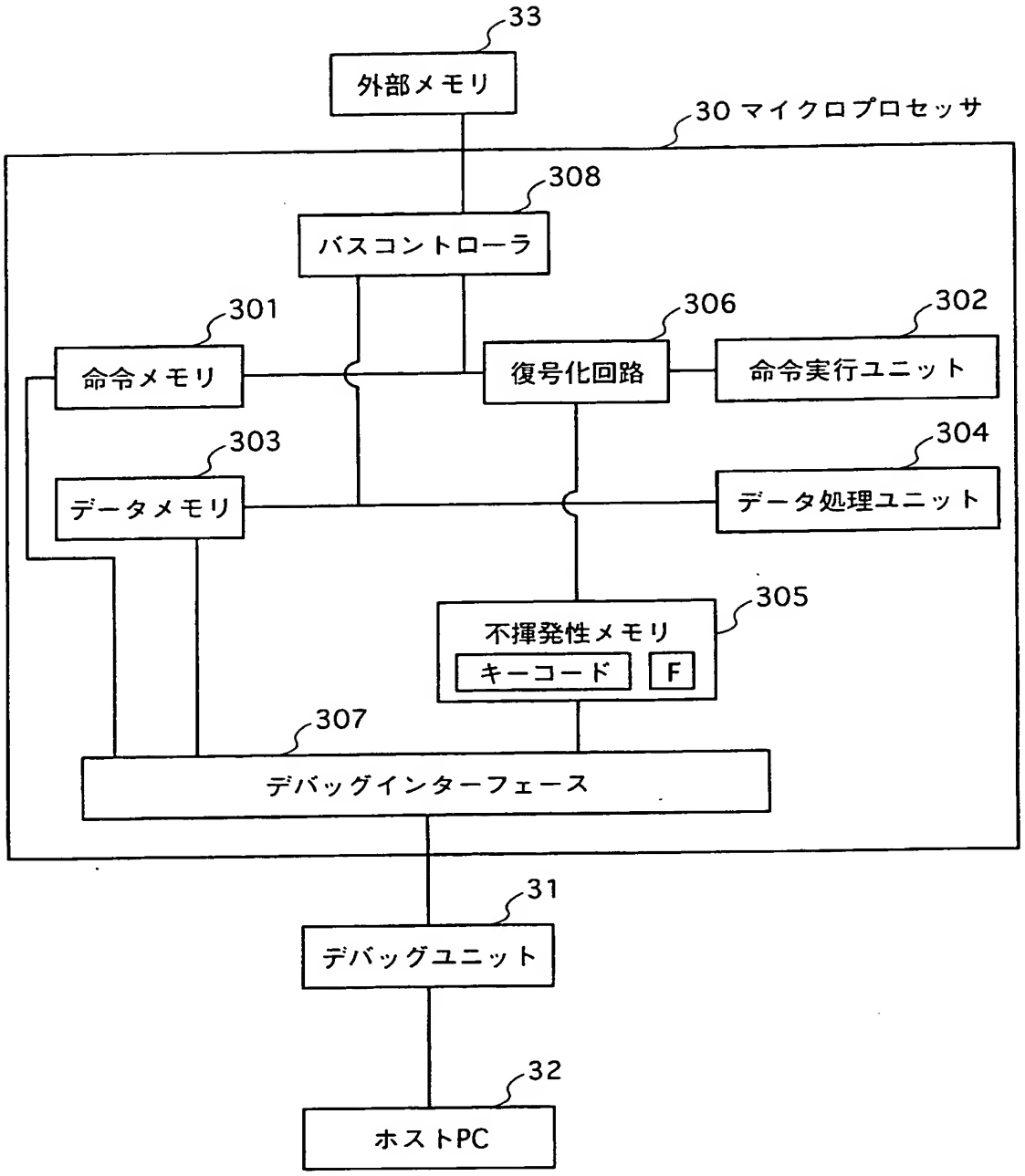
【図６】


21
デバッグ
ユニット
マイクロ
プロセッサ20へ
暗号文
暗号文
キーコード
コマンド
22 ホストPC
229
227
225
226
228
221
暗号部
復号部
キーコード入力部
コマンド入力部
命令・データ入力部
表示部
222
224
232
234
オブジェクト
ファイル
暗号部
暗号化
オブジェクト
ファイル
231
223
235
ソース
ファイル
コンパイル
アセンブル
リンク
処理部
233
キーコード入力部

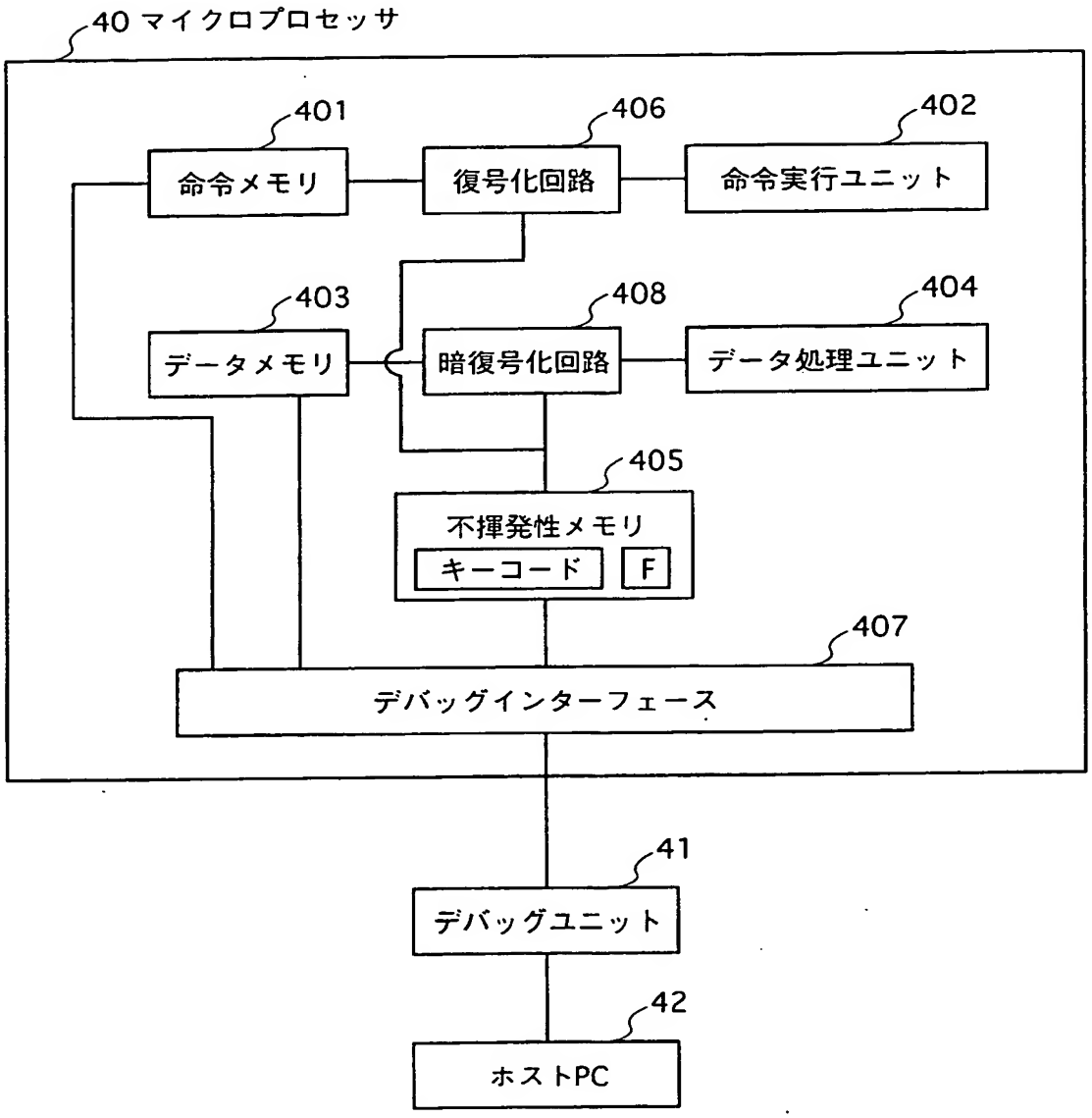
【図７】


「終了」
終了
S231
S232
S233
「データ書込み」
データの入力を受け付ける
受け付けたデータを出力する
データをデータメモリに格納する
S221
S222
「データ表示」
データメモリからデータを読み出す
データを受け取り表示する
A1
A2
S206
S207
S208
S209
「命令書込み」
命令の入力を受け付ける
キーコードを用いて暗号化する
暗号化命令を出力する
命令メモリに格納する
S201
S202
S203
「命令表示」
命令メモリから暗号化命令を読み出す
暗号化命令を受け取りキーコードを用いて復号する
復号した命令を表示する

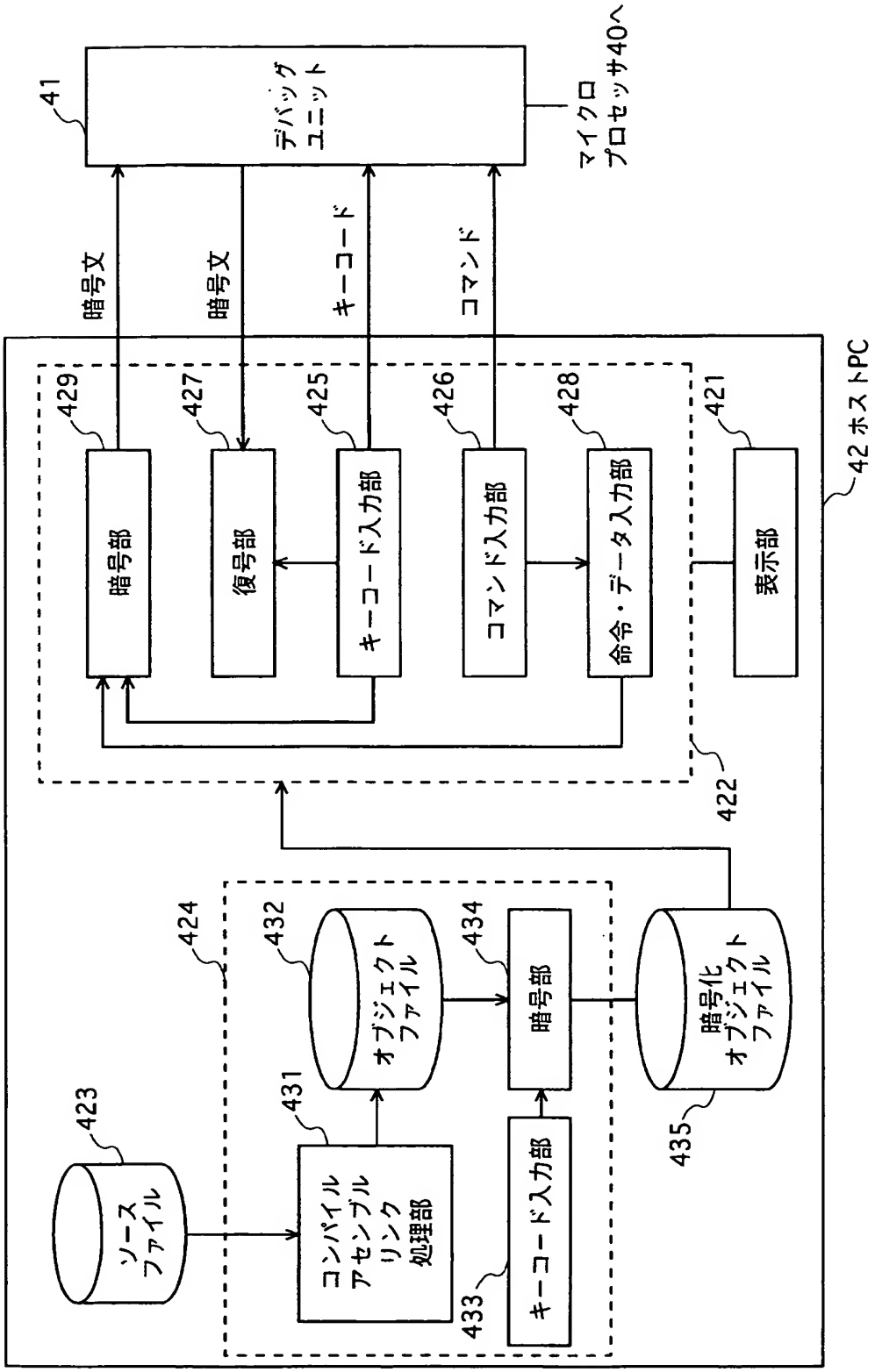
【図８】


33
外部メモリ
30 マイクロプロセッサ
308
バスコントローラ
301
命令メモリ
306
復号化回路
302
命令実行ユニット
303
データメモリ
304
データ処理ユニット
305
不揮発性メモリ
キーコード
F
307
デバッグインターフェース
31
デバッグユニット
32
ホストPC

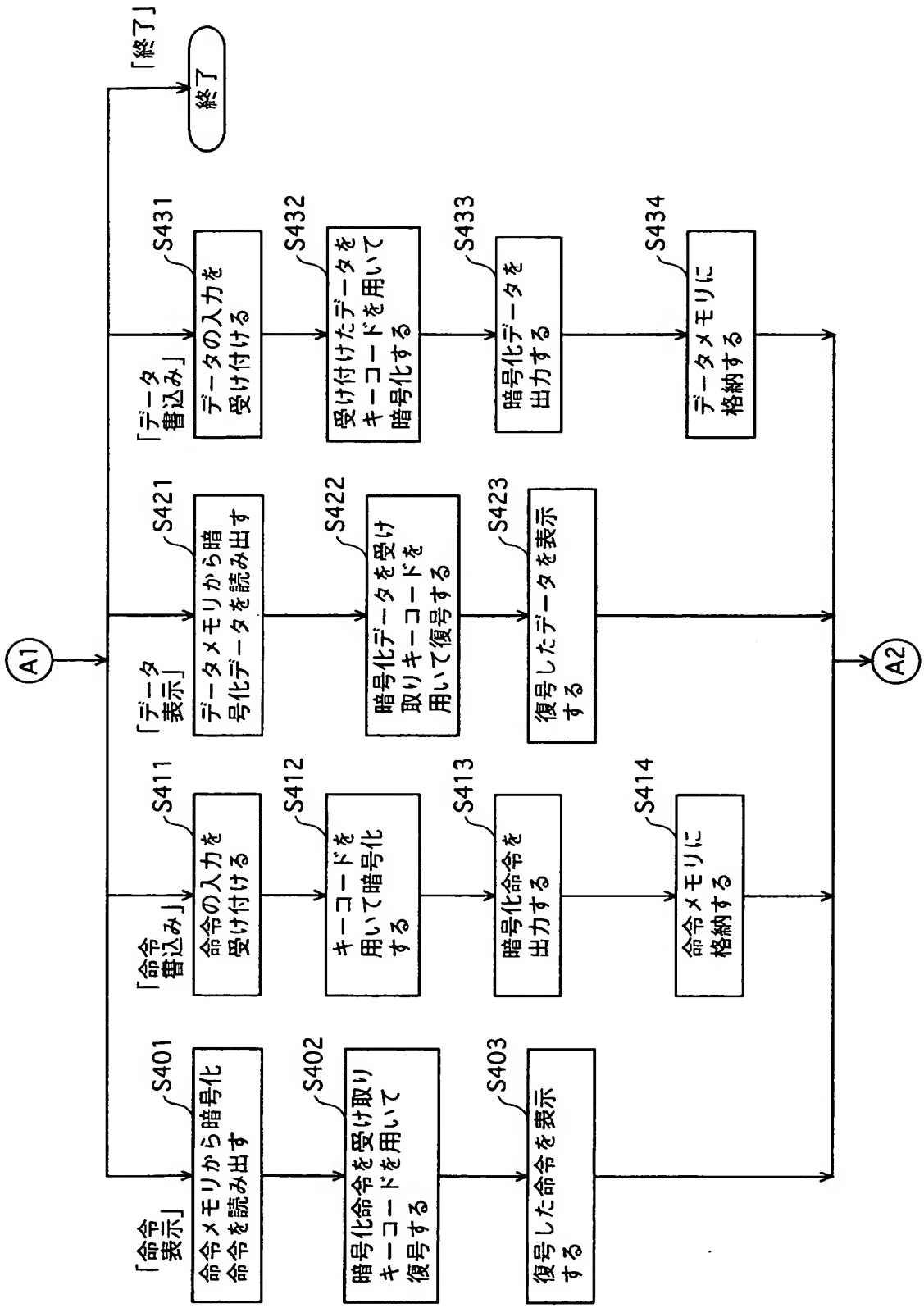
【図９】


40 マイクロプロセッサ
401
命令メモリ
406
復号化回路
402
命令実行ユニット
403
データメモリ
408
暗復号化回路
404
データ処理ユニット
405
不揮発性メモリ
キーコード
F
407
デバッグインターフェース
41
デバッグユニット
42
ホストPC

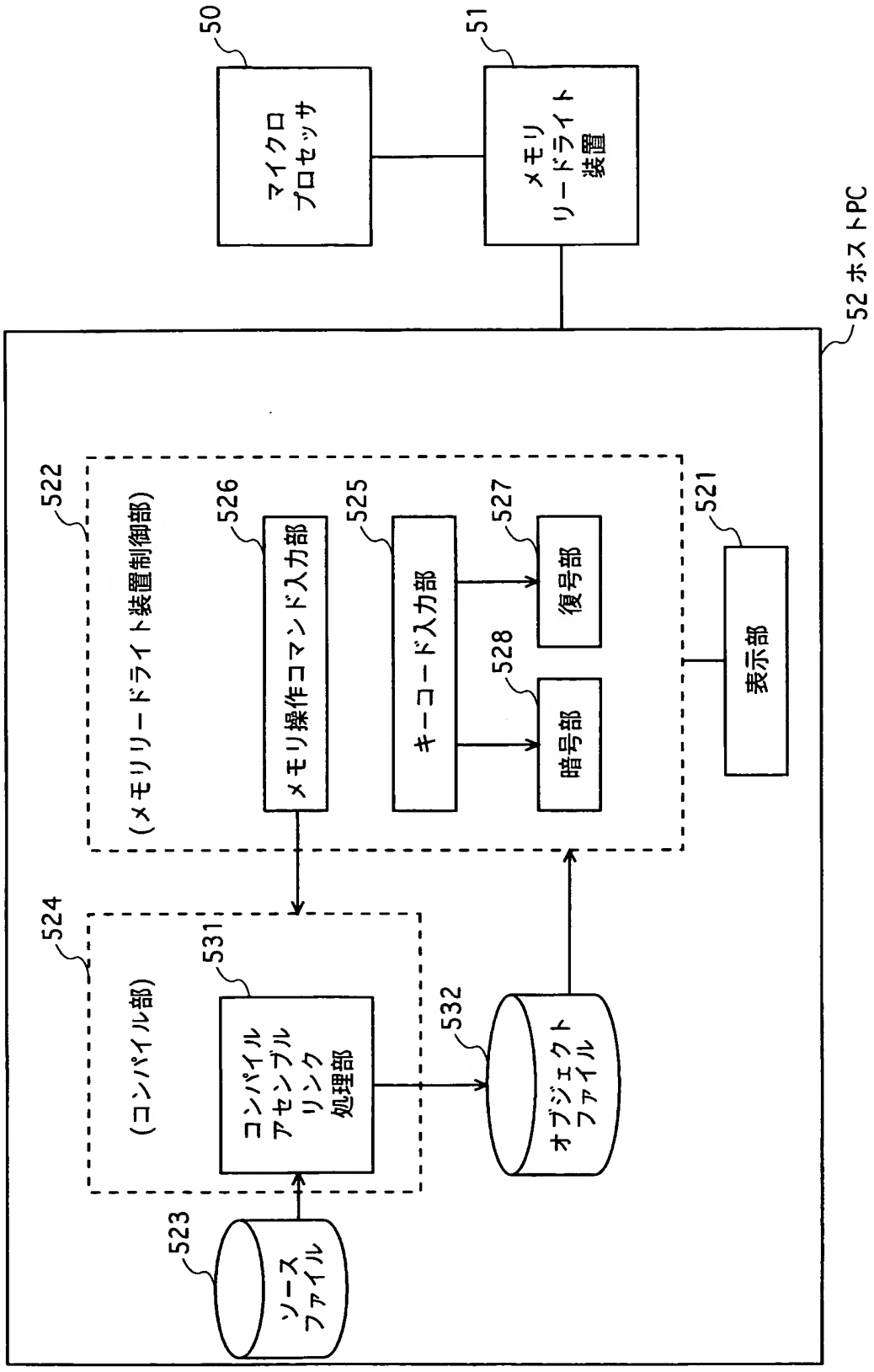
【図１０】


41
デバッグ
ユニット
マイクロ
プロセッサ40へ
暗号文
暗号文
キーコード
コマンド
429
427
425
426
428
421
暗号部
復号部
キーコード入力部
コマンド入力部
命令・データ入力部
表示部
42 ホストPC
422
424
432
434
オブジェクト
ファイル
暗号部
暗号化
オブジェクト
ファイル
423
431
435
ソース
ファイル
コンパイル
アセンブル
リンク
処理部
433
キーコード入力部

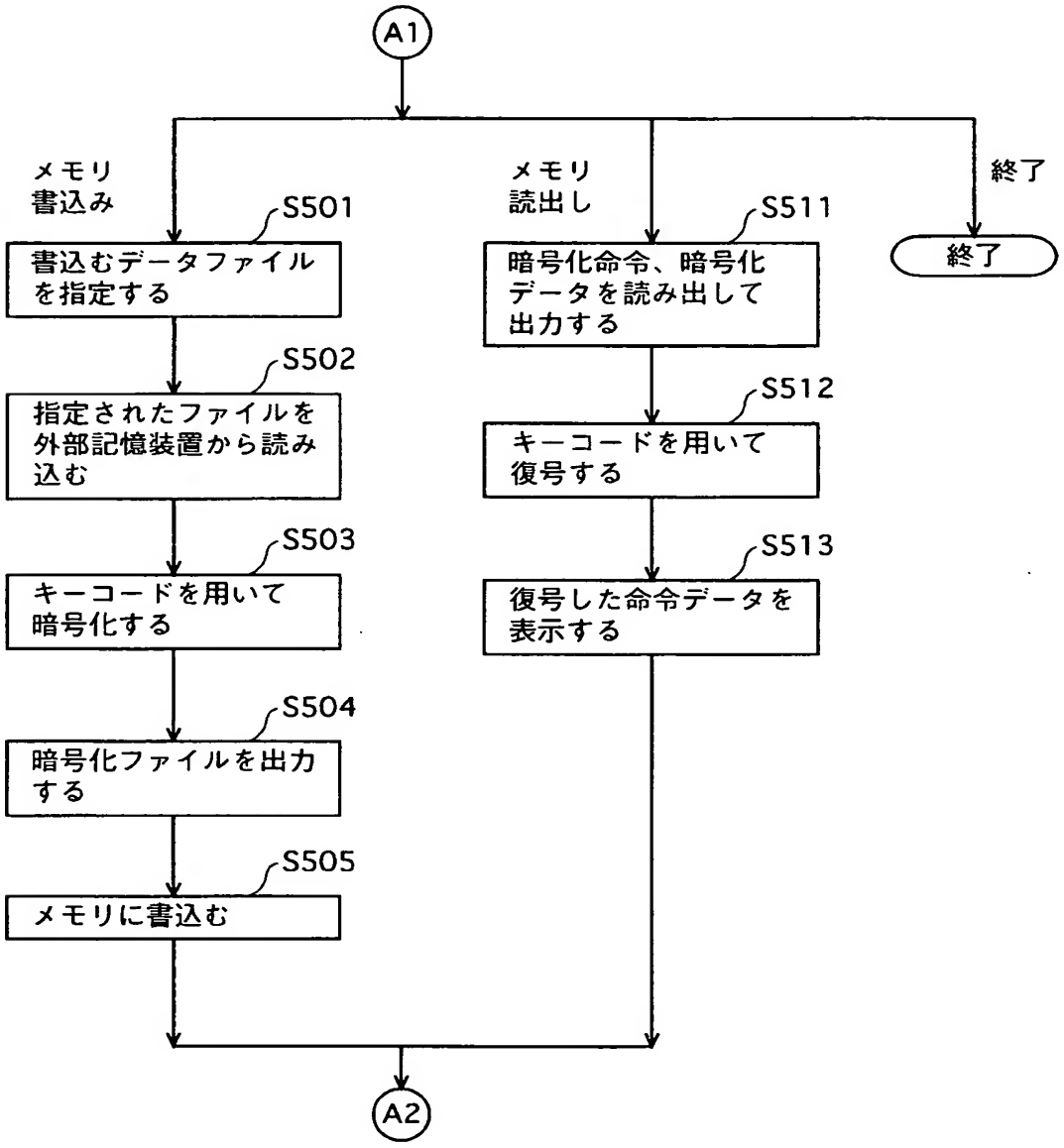
【図１１】


「終了」
終了
「データ書込み」
S431
データの入力を受け付ける
S432
受け付けたデータをキーコードを用いて暗号化する
S433
暗号化データを出力する
S434
データメモリに格納する
「データ表示」
S421
データメモリから暗号化データを読み出す
S422
暗号化データを受け取りキーコードを用いて復号する
S423
復号したデータを表示する
「命令書込み」
S411
命令の入力を受け付ける
S412
キーコードを用いて暗号化する
S413
暗号化命令を出力する
S414
命令メモリに格納する
「命令表示」
S401
命令メモリから暗号化命令を読み出す
S402
暗号化命令を受け取りキーコードを用いて復号する
S403
復号した命令を表示する
A1
A2

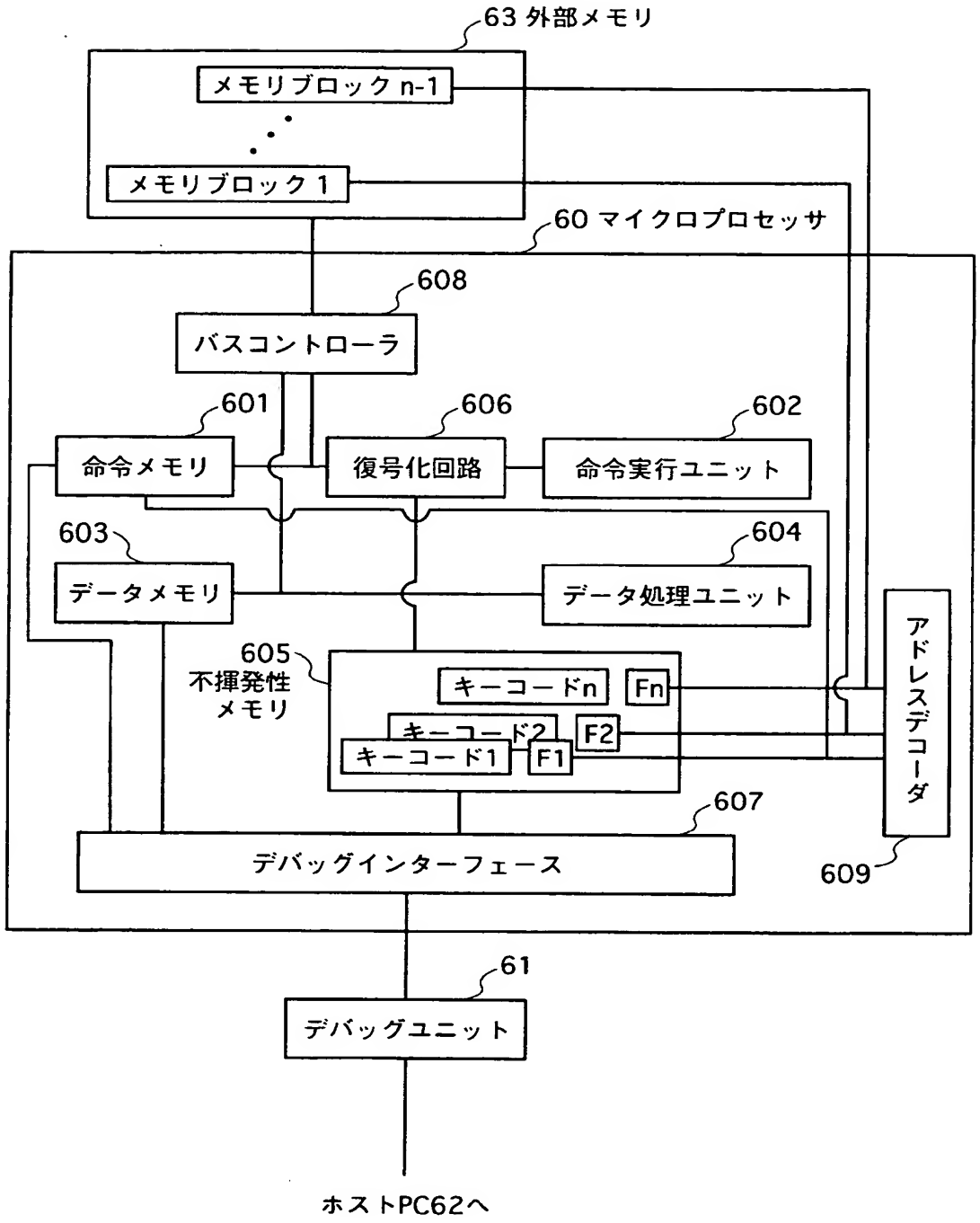
【図１２】


50
マイクロプロセッサ
51
メモリリードライト装置
52 ホストPC
522
(メモリリードライト装置制御部)
526
メモリ操作コマンド入力部
525
キーコード入力部
527
復号部
528
暗号部
521
表示部
524
(コンパイル部)
531
コンパイルアセンブルリンク処理部
532
オブジェクトファイル
523
ソースファイル

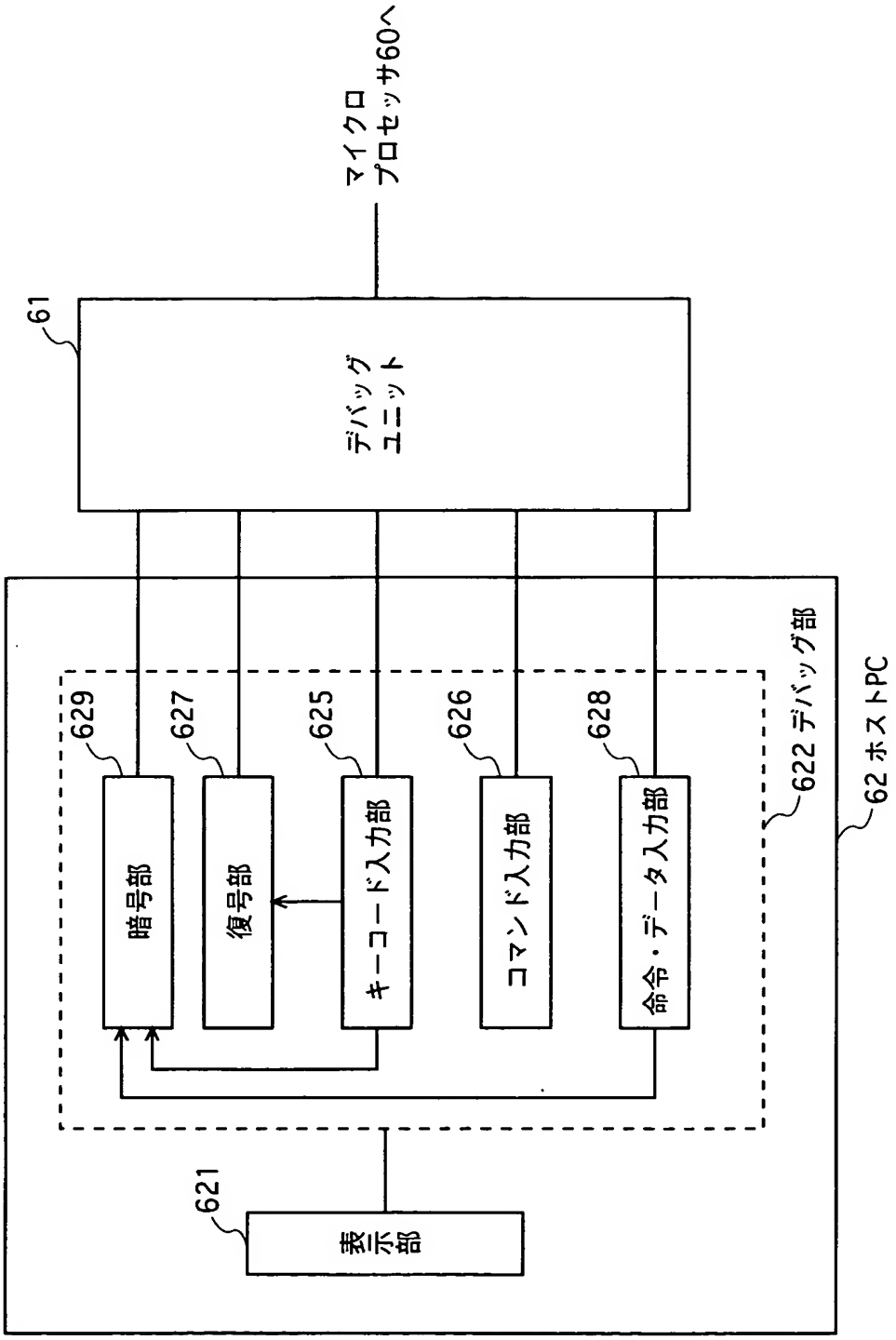
【図１３】


A1
メモリ
書込み
S501
書込むデータファイル
を指定する
S502
指定されたファイルを
外部記憶装置から読み
込む
S503
キーコードを用いて
暗号化する
S504
暗号化ファイルを出力
する
S505
メモリに書込む
メモリ
読出し
S511
暗号化命令、暗号化
データを読み出して
出力する
S512
キーコードを用いて
復号する
S513
復号した命令データを
表示する
終了
終了
A2

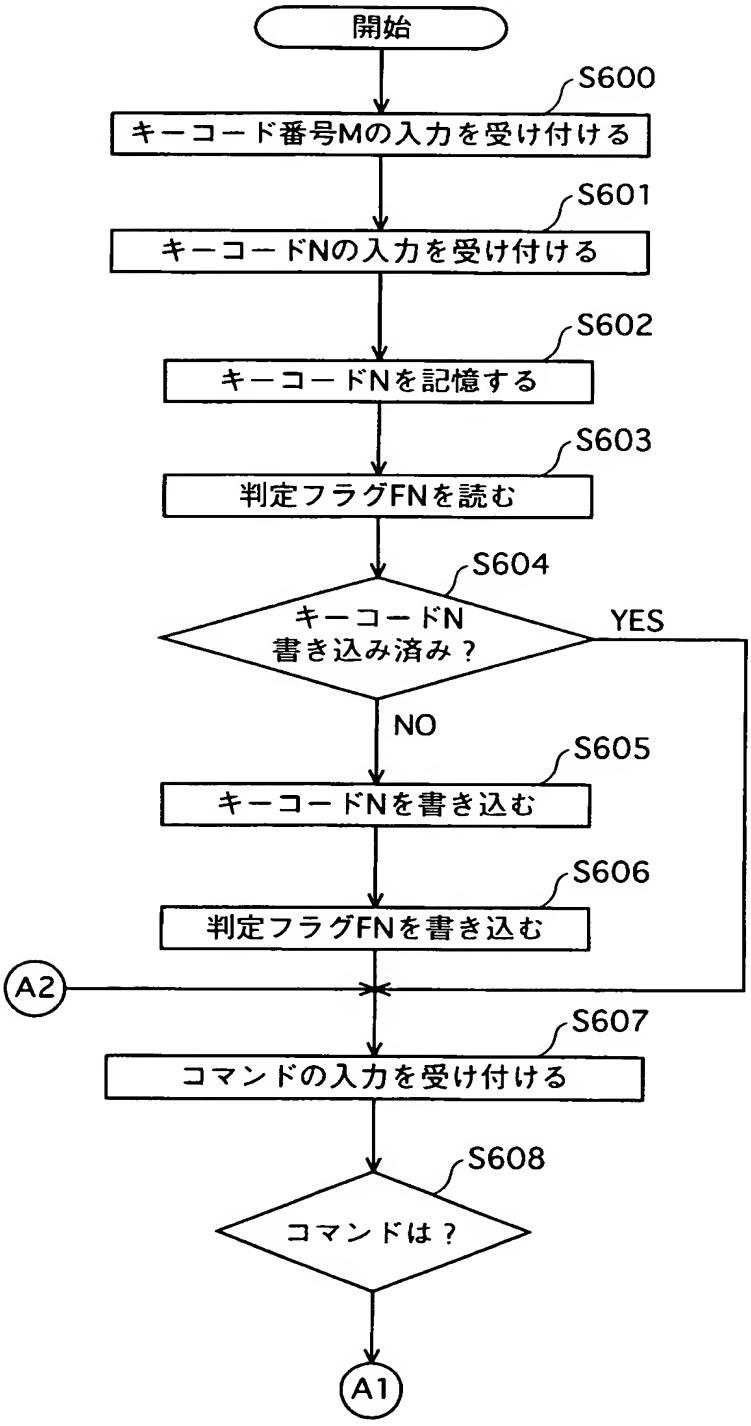
【図１４】


63 外部メモリ
メモリブロック n-1
メモリブロック 1
60 マイクロプロセッサ
608
バスコントローラ
601
命令メモリ
606
復号化回路
602
命令実行ユニット
603
データメモリ
604
データ処理ユニット
605
不揮発性
メモリ
キーコードn
Fn
キーコード2
F2
キーコード1
F1
607
デバッグインターフェース
609
アドレスデコーダ
61
デバッグユニット
ホストPC62へ

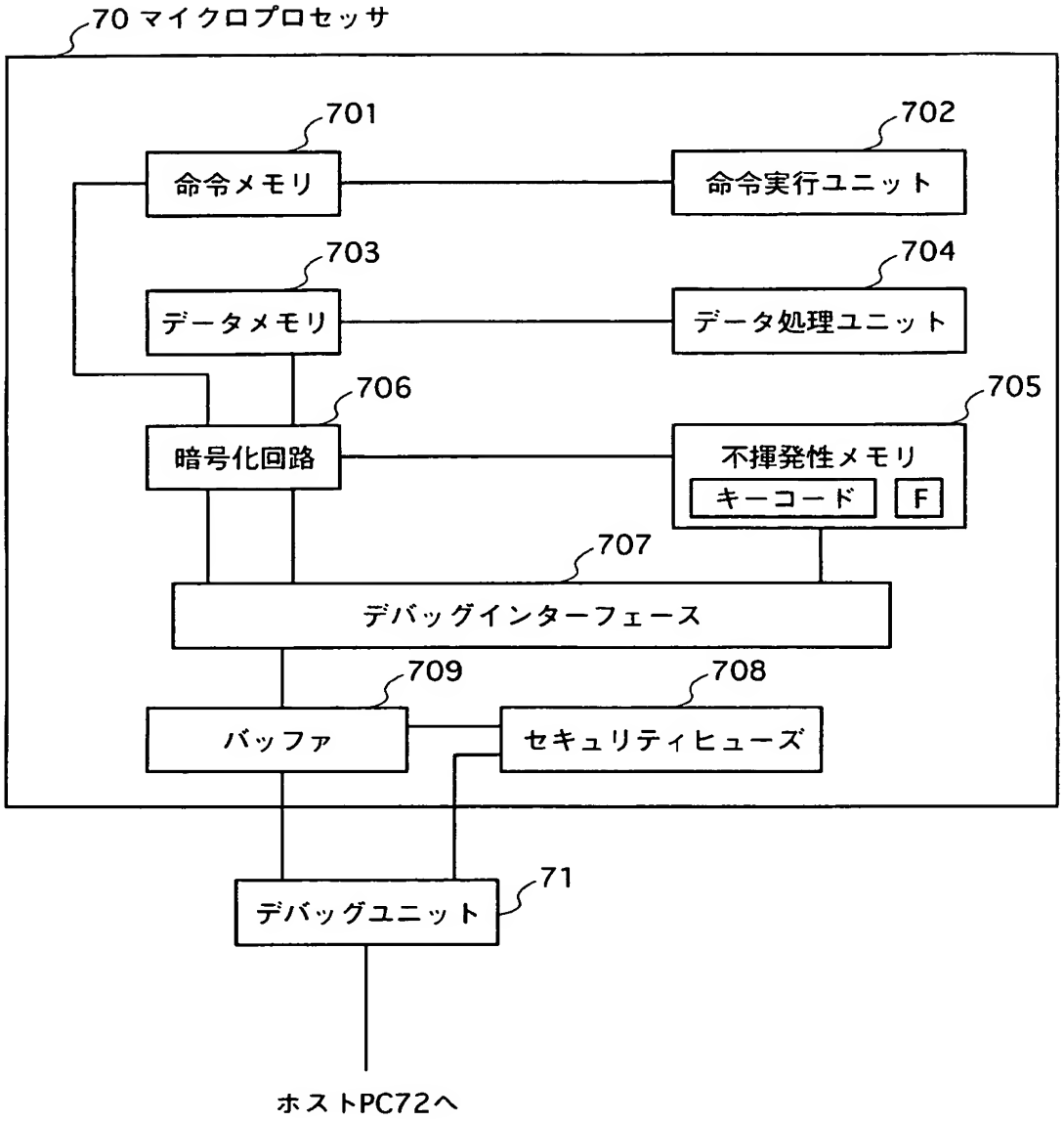
【図１５】


マイクロプロセッサ60へ
61
デバッグユニット
62 ホストPC
622 デバッグ部
629
627
625
626
628
暗号部
復号部
キーコード入力部
コマンド入力部
命令・データ入力部
621
表示部

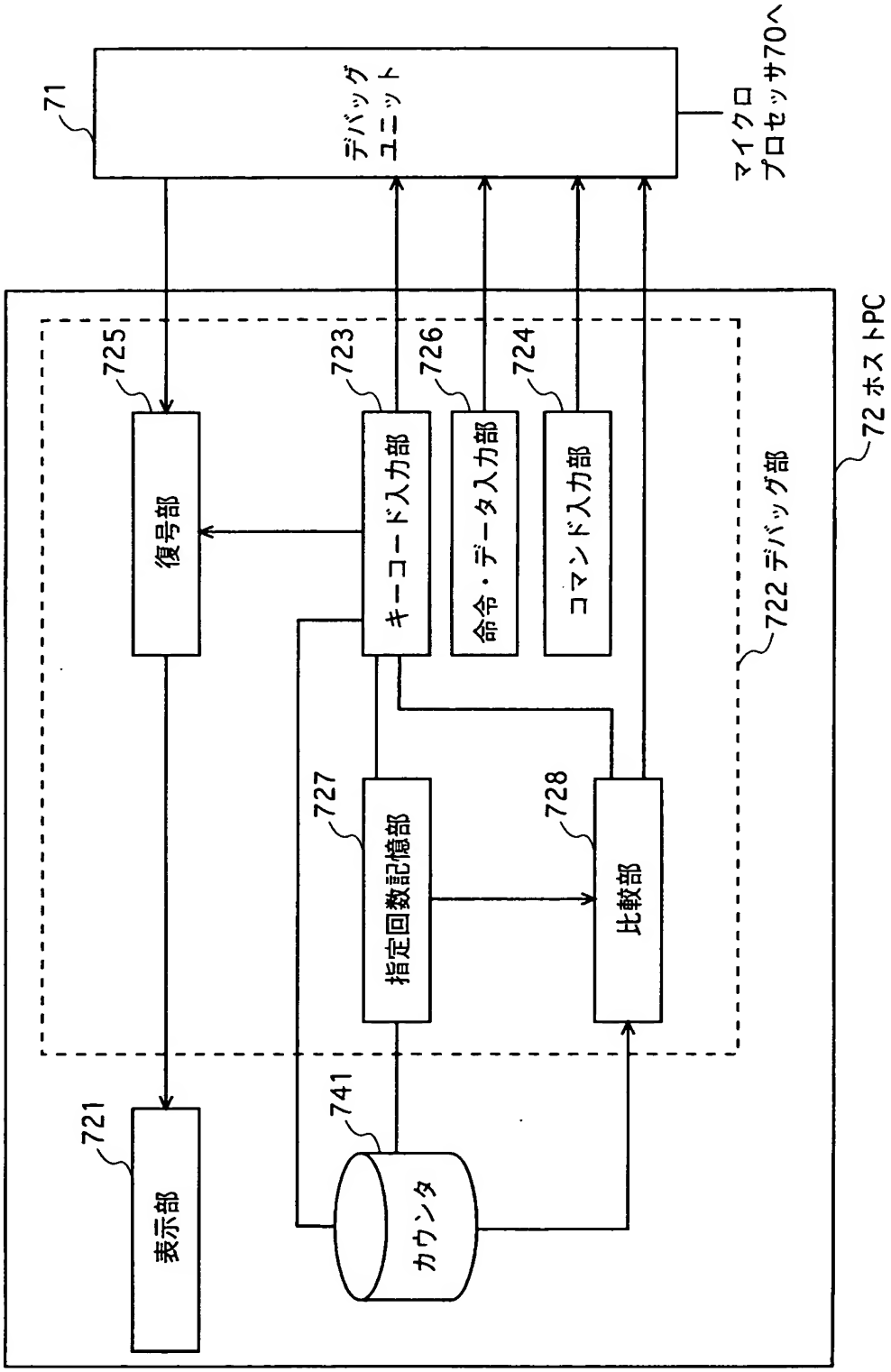
【図１６】


開始
S600
キーコード番号Mの入力を受け付ける
S601
キーコードNの入力を受け付ける
S602
キーコードNを記憶する
S603
判定フラグFNを読む
S604
キーコードN
書き込み済み？
YES
NO
S605
キーコードNを書き込む
S606
判定フラグFNを書き込む
A2
S607
コマンドの入力を受け付ける
S608
コマンドは？
A1

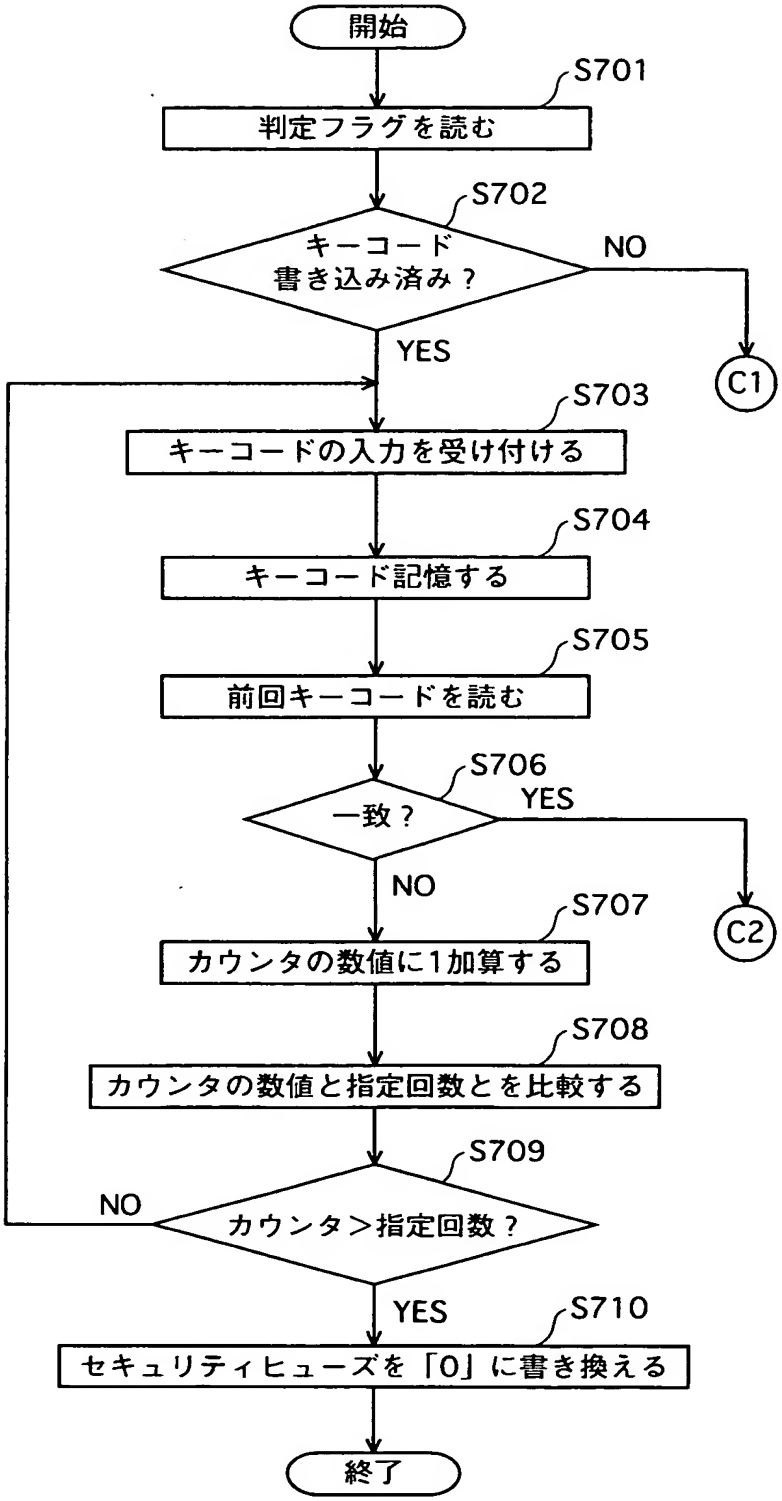
【図１７】


70 マイクロプロセッサ
701
命令メモリ
702
命令実行ユニット
703
データメモリ
704
データ処理ユニット
706
暗号化回路
705
不揮発性メモリ
キーコード
F
707
デバッグインターフェース
709
バッファ
708
セキュリティヒューズ
71
デバッグユニット
ホストPC72へ

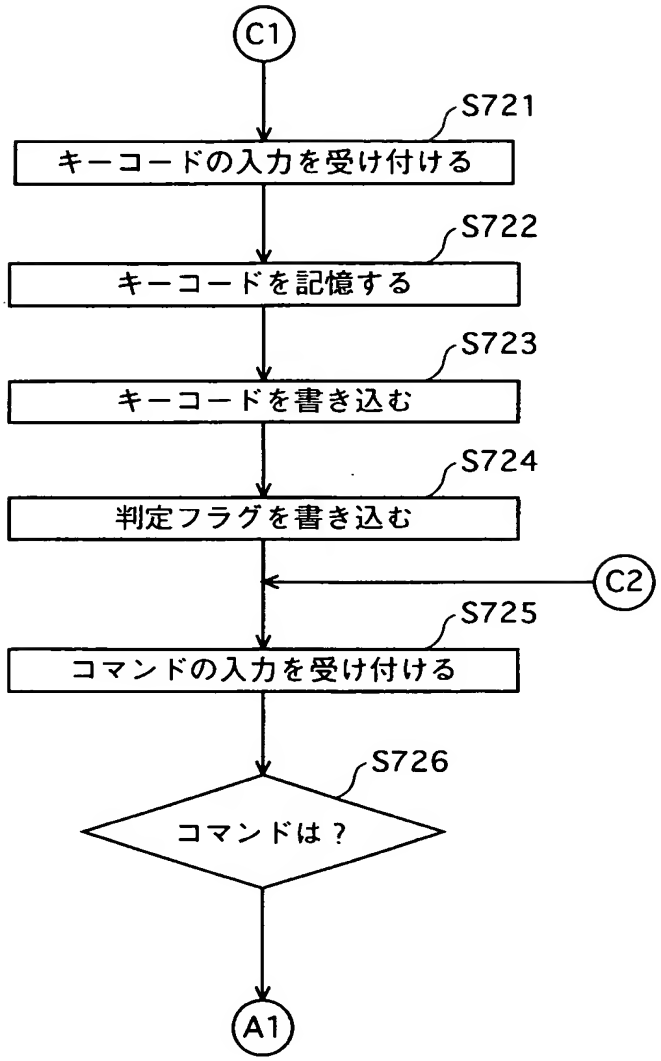
【図１８】


71
デバッグユニット
マイクロプロセッサ70へ
72 ホストPC
722 デバッグ部
725
723
726
724
復号部
キーコード入力部
命令・データ入力部
コマンド入力部
727
728
指定回数記憶部
比較部
721
741
表示部
カウンタ

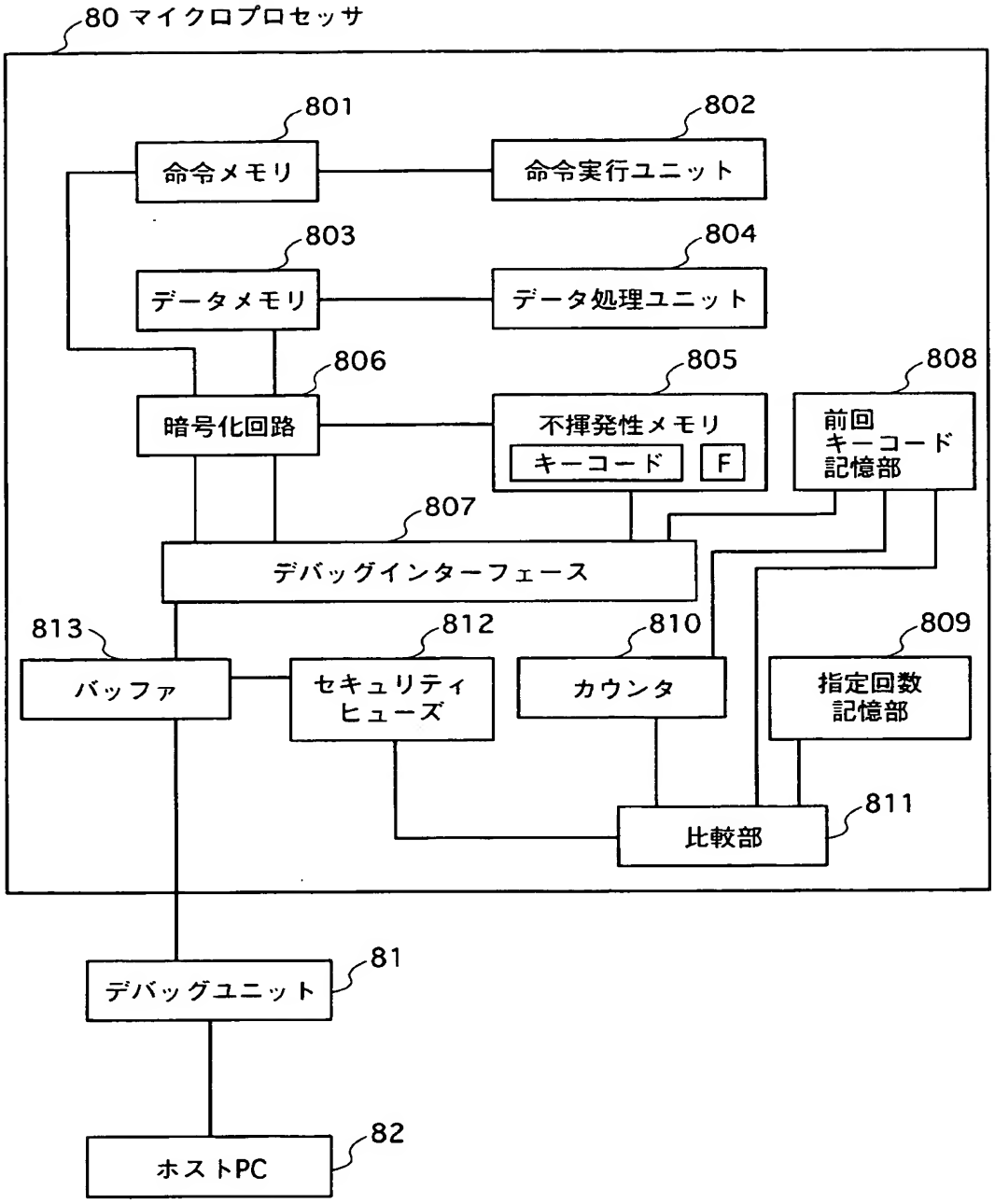
【図１９】


開始
S701
判定フラグを読む
S702
キーコード
書き込み済み？
NO
YES
C1
S703
キーコードの入力を受け付ける
S704
キーコード記憶する
S705
前回キーコードを読む
S706
一致？
YES
NO
C2
S707
カウンタの数値に1加算する
S708
カウンタの数値と指定回数とを比較する
S709
NO
カウンタ＞指定回数？
YES
S710
セキュリティヒューズを「0」に書き換える
終了

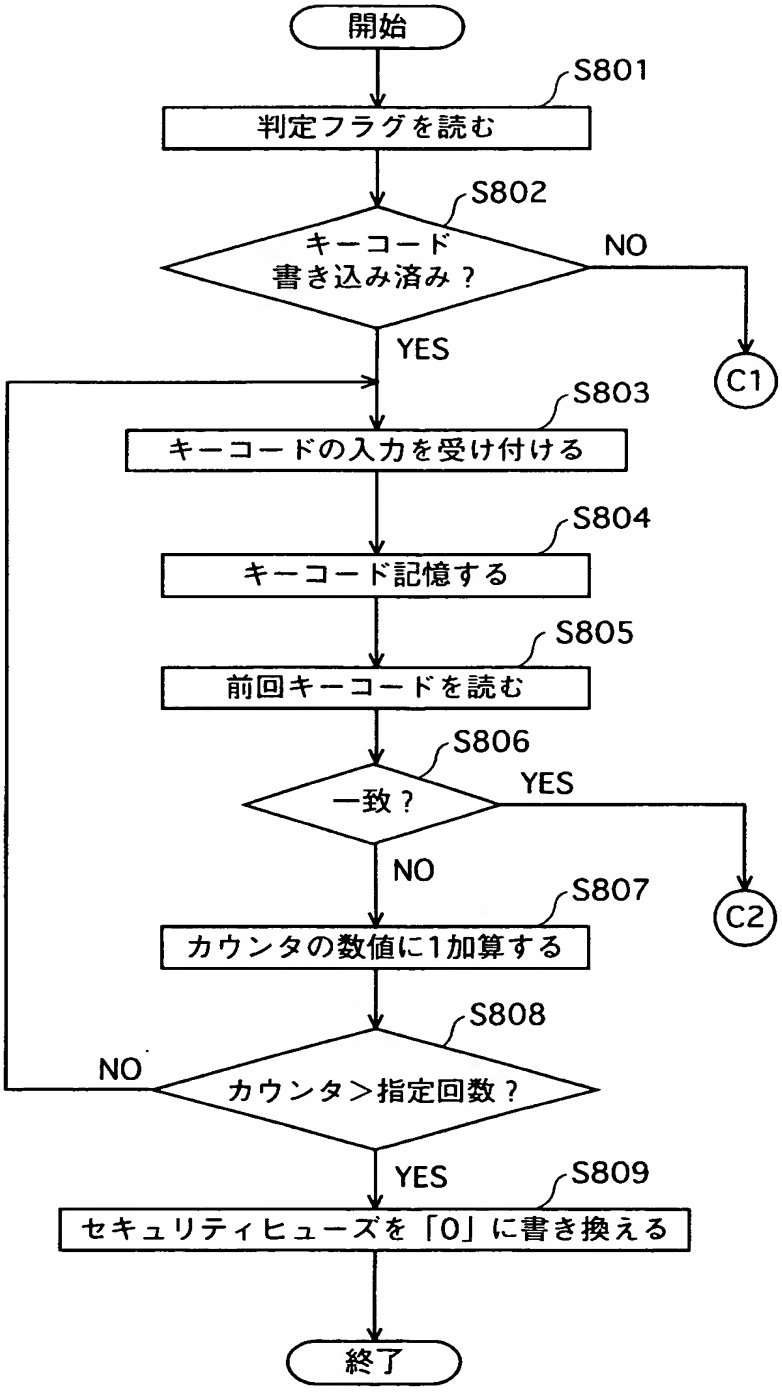
【図２０】


C1
S721
キーコードの入力を受け付ける
S722
キーコードを記憶する
S723
キーコードを書き込む
S724
判定フラグを書き込む
C2
S725
コマンドの入力を受け付ける
S726
コマンドは？
A1

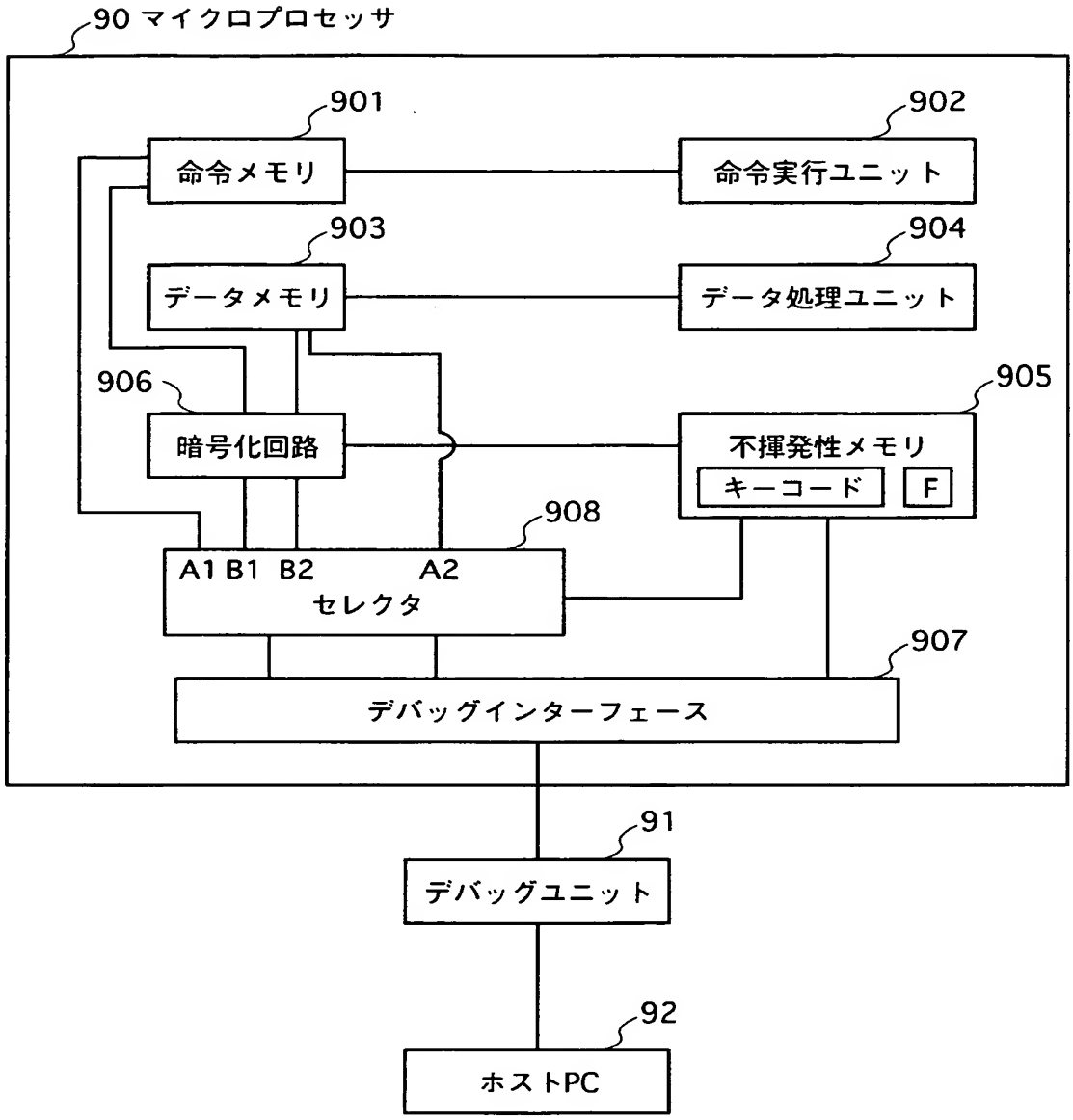
【図２１】


80 マイクロプロセッサ
801
命令メモリ
802
命令実行ユニット
803
データメモリ
804
データ処理ユニット
806
暗号化回路
805
不揮発性メモリ
キーコード
F
808
前回
キーコード
記憶部
807
デバッグインターフェース
813
バッファ
812
セキュリティ
ヒューズ
810
カウンタ
809
指定回数
記憶部
811
比較部
81
デバッグユニット
82
ホストPC

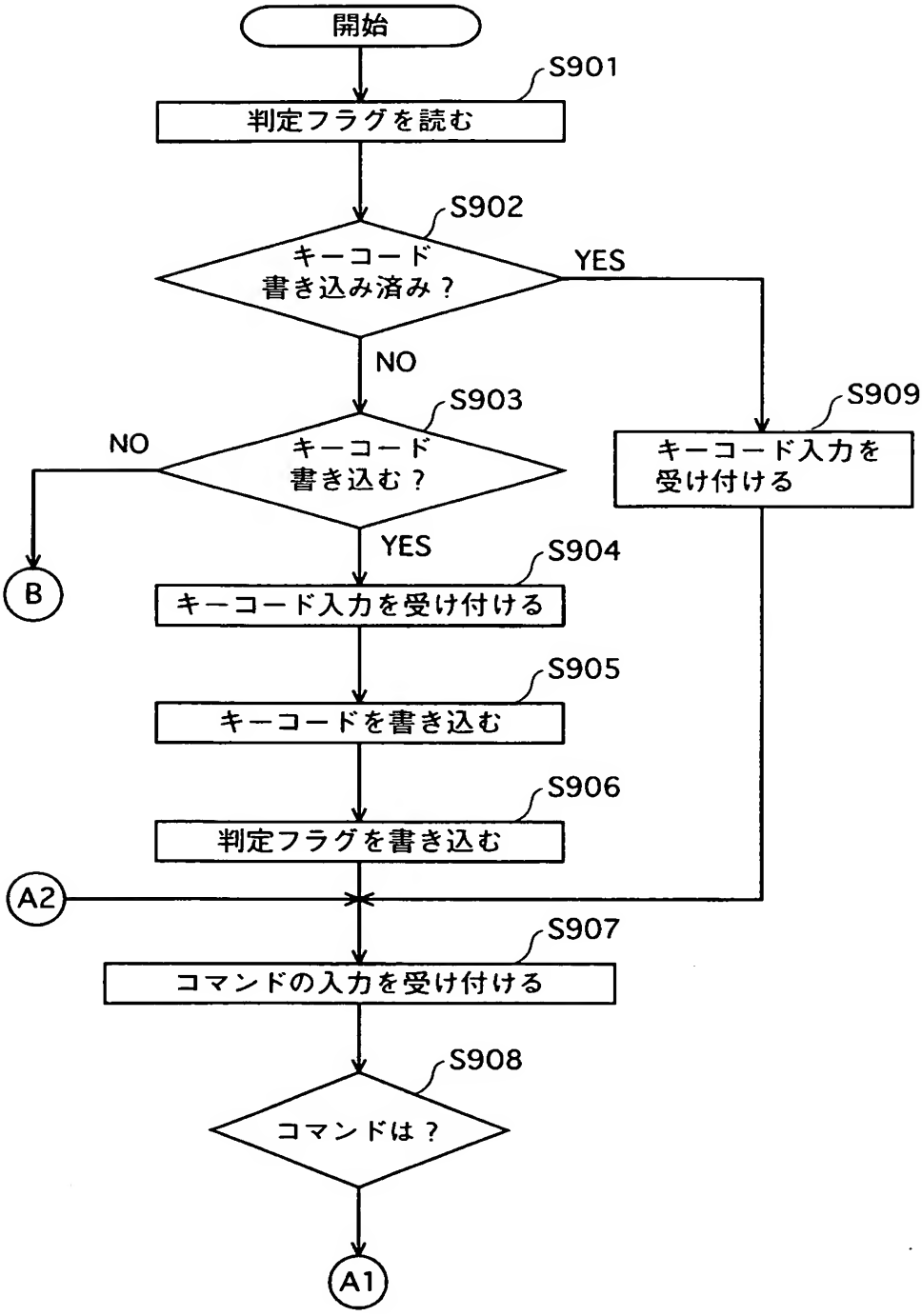
【図２２】


開始
S801
判定フラグを読む
S802
キーコード
書き込み済み？
NO
YES
C1
S803
キーコードの入力を受け付ける
S804
キーコード記憶する
S805
前回キーコードを読む
S806
一致？
YES
NO
C2
S807
カウンタの数値に1加算する
S808
NO
カウンタ＞指定回数？
YES
S809
セキュリティヒューズを「0」に書き換える
終了

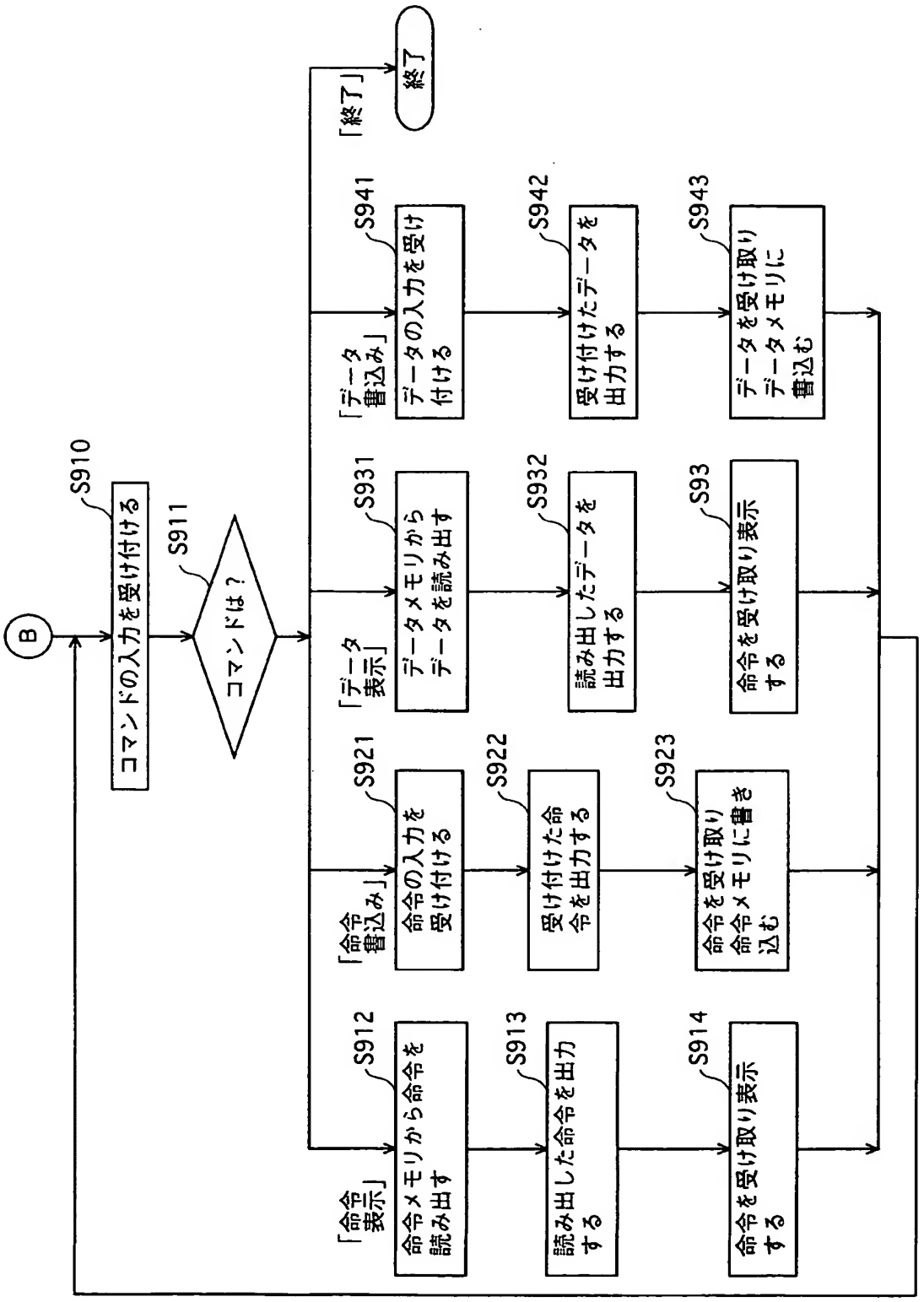
【図２３】


90 マイクロプロセッサ
901
命令メモリ
902
命令実行ユニット
903
データメモリ
904
データ処理ユニット
906
暗号化回路
905
不揮発性メモリ
キーコード
F
908
A1 B1 B2 A2
セレクタ
907
デバッグインターフェース
91
デバッグユニット
92
ホストPC

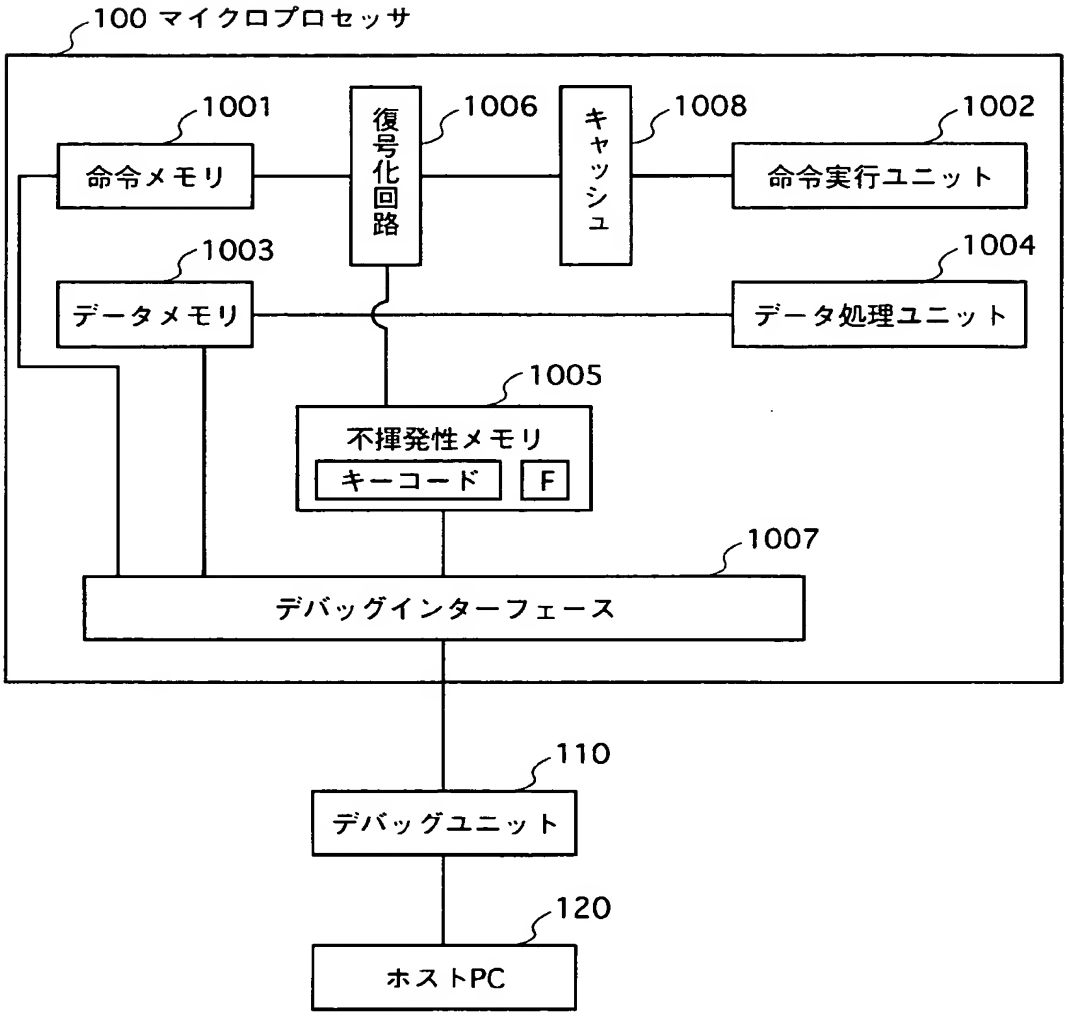
【図２４】


開始
S901
判定フラグを読む
S902
キーコード
書き込み済み？
YES
NO
S903
キーコード
書き込む？
NO
YES
S909
キーコード入力を
受け付ける
B
S904
キーコード入力を受け付ける
S905
キーコードを書き込む
S906
判定フラグを書き込む
A2
S907
コマンドの入力を受け付ける
S908
コマンドは？
A1

【図２５】


B
S910
コマンドの入力を受け付ける
S911
コマンドは？
「命令表示」
S912
命令メモリから命令を読み出す
S913
読み出した命令を出力する
S914
命令を受け取り表示する
「命令書込み」
S921
命令の入力を受け付ける
S922
受け付けた命令を出力する
S923
命令を受け取り命令メモリに書き込む
「データ表示」
S931
データメモリからデータを読み出す
S932
読み出したデータを出力する
S93
命令を受け取り表示する
「データ書込み」
S941
データの入力を受け付ける
S942
受け付けたデータを出力する
S943
データを受け取りデータメモリに書込む
「終了」
終了

【図２６】


100 マイクロプロセッサ
1001
命令メモリ
復号化回路
1006
キャッシュ
1008
1002
命令実行ユニット
1003
データメモリ
1004
データ処理ユニット
1005
不揮発性メモリ
キーコード
F
1007
デバッグインターフェース
110
デバッグユニット
120
ホストPC

【書類名】　要約書

【要約】

【課題】　マイクロプロセッサのデバッグと内部情報のセキュリティの維持とを両立するデバッグシステムを提供する。

【解決手段】　マイクロプロセッサは、ホストＰＣ上でユーザから入力されたキーコードを内部に記憶し、当該キーコードを用いて命令やデータを暗号化してホストＰＣへ送出する。悪意のあるユーザが、マイクロプロセッサをデバッグユニットに接続して暗号化命令及び暗号化データを取得した場合であっても、前記キーコードを知らなければ暗号化命令及び暗号化データを復号することはできない。

【選択図】　図１

特願２００３－０７６１４５

出　願　人　履　歴　情　報

識別番号　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社